Abstract Algebra and Number Theory

Davide Galassi <davxy@datawok.net>

v0.1.0

Table of Contents

Equivalence Classes

Equivalence relation. A binary relation ~ on a set *S* that for any *a*, *b* and *c* in *S* it is:

- **Reflexive**: a ~ a
- **Symmetric**: a ~ b then b ~ a
- **Transitive**: a ~ b and b ~ c then a ~ c

When *S* has an equivalence relation on it, then *S* can be partitioned into subsets, called **equivalence classes**. Two elements are in the same equivalence class if they are equivalent.

Proposition. *If two equivalence classes have any elements at all in common, then they coincide.*

Proof. Assume that $c \in S$ belongs to both $A \subseteq S$ and $B \subseteq S$. In other words $c \sim a \ \forall a \in A$ and $c \sim b \ \forall b \in B$. By the symmetric property $c \sim a \rightarrow a \sim c$ and for the transitive property $a \sim c \ \wedge \ c \sim b \ \rightarrow \ a \sim b$. Because the result is valid for any two arbitrary elements of *A* and *B* the two sets coincide.

Example. One of the most popular equivalence relation is the definition of the set of **rational numbers**. Two rational numbers (*a*,*b*) and (*c*,*d*) are equivalent *iff ad=bc.*
Reflexivity: (a,b)~(a,b) . Proof: ab = ab
Symmetry: (a,b)~(c,d) → (c,d)~(a,b). Proof: ad = bc → cb = da
Transitivity: (a,b)~(c,d) and (c,d)~(e,f)→ (a,b)~(e,f). Proof: ad=bc and cf=de → adcf=bcde → af=be.

Induction

Basic proof method for facts about natural numbers. Allows to obtain, in a finite number of steps, proofs of statements about all the numbers in the infinite set $\mathbb{N}$.

Well Ordering Principle. *Any nonempty set of natural numbers has a least element.*

Proof. Let *L* be a set of natural numbers with no last element. Let $P(n)$ be the statement "Every number in *L* is greater than *n*". If $P(n)$ is true then *n* is not in *L*. By showing that $P(n)$ is true for all *n*, we show that *L* is empty.

$P(1)$ is true. If not, then 1 is the least element of L since all natural numbers are ≥ 1. Assume that $P(k)$ is true. If $P(k+1)$ is false then L contains some number $\leq k+1$. Since $P(k)$ is true, every number in L is $>k$, but then $k+1$ should be in L and is the least element. This is impossible because L has no least element. Thus if $P(k)$ is true then $P(k+1)$ should be true. By induction P is true for every $n \in \mathbb{N}$ thus L is empty.

Induction. Let n_0 be a fixed integer and let $P(n)$ be a statement which makes sense for every integer $n \geq n_0$. Then $P(n)$ is true for all $n \geq n_0$ if the following two statements are true:

- *Base case*: $P(n_0)$ is true;
- *Induction step*: for all $k \geq n_0$, if $P(k)$ is true then $P(k+1)$ is true.

Proof. Let $L = \{x : x \geq n_0 \wedge P(x) = false\}$. Assuming $L \neq \emptyset$, then for the WOP there is a least element $m \in L$, such that $P(m)$ is false. For the base case $P(n_0)$ is true thus $m > n_0$. Since m is the minimum of L then $m-1 \notin L$ and thus $P(m-1)$ is true. But then for the induction step $P(m)$ is true. Thus m cannot be part of L. The contradiction indicates that L cannot have a last element, thus is empty.

The rationale behind the induction is that if the base case and the induction step are both true, then for any $n > n_0$, one can prove $P(n)$ in $n - n_0$ steps.

Because WOP implies mathematical induction and mathematical induction implies WOP, the two statements are **equivalent**. To break the **cyclic dependency**, induction is usually proposed as an axiom of the natural numbers (*Peano* axioms).

Complete induction. Let n_0 be a fixed integer and let $P(n)$ be a statement for which makes sense for every integer $n \geq n_0$. Then $P(n)$ is true for all $n \geq n_0$ if the following two statements are true:

- *Base case*: $P(n_0)$ is true;
- *Induction step*: for all $m > n_0$, if $P(k)$ is true for all k with $n_0 \leq k < m$, then $P(m)$ is true.

Complete induction allows to assume more than ordinary induction. In the attempt to prove $P(m)$ with ordinary induction you are only allowed to assume $P(m-1)$.

Proof. Let $L = \{x : x \geq n_0 \wedge P(x) = false\}$. Assuming $L \neq \emptyset$, then for the WOP there is a least element $m \in L$. For the base case $P(n_0)$ is true thus $m > n_0$ and also $P(k)$ is true for every k such that $n_0 \leq k < m$. But then for the induction step $P(m)$ is true, thus m cannot be part of L. The contradiction indicates that L cannot have a last element, thus is empty.

Theorem. *If* $P(n)$ *can be proved by ordinary induction then it can be proved by complete induction.*

Proof. If we can prove $P(n)$ assuming only $P(n-1)$ then we can prove it by assuming $P(k)$ for all $n_0 \leq k < n$ since it includes $P(n-1)$.

Theorem. *If* $P(n)$ *can be proved by complete induction then it can be proved by ordinary induction.*

Proof. Consider the new statement $Q(n)$: " $P(k)$ *is true for all k,* $n_0 \leq k \leq n$ ". Note that if $Q(n)$ is true, then $P(n)$ is true. We prove that $Q(n)$ is true for all $n \geq n_0$ by ordinary induction.

Base case: $Q(n_0)$ is equivalent to $P(n_0)$, thus if $Q(n_0)$ is true then $P(n_0)$ is true.

Induction step: we need to show that if $Q(n-1)$ is true then $Q(n)$ is true. If $Q(n-1)$ is true then $P(k)$ is true for all k with $n_0 \leq k \leq n-1$. For complete induction hypothesis then $P(n)$ is true. But then $P(k)$ is true for all k with $n_0 \leq k \leq n$ and so $Q(n)$ is true. Thus, by ordinary induction, $Q(n)$ is true for all $n \geq n_0$ and consequently $P(n)$ is true for all $n \geq n_0$.

Corollary. *Ordinary and complete induction are equivalent.*

Recursive functions

The induction principle can be used to define a function with domain in $\mathbb{N}$.

If we can define $f(n_0)$ with $n_0 \in \mathbb{N}$ and given the values of $f(k)$, $n_0 \leq k < n$, we can define $f(n)$. Then we can define the function $f(n)$ for each natural number $n \geq n_0$.

In other words, for $n \in \mathbb{N}$ we can define $f(n)$ respect to the values of $f(k)$ with $n_0 \leq k < n$.

Binomial Theorem

Pascal triangle

Lets define $c(n,r)$ as the function defining the element of the triangle that belongs to the row *n* and the column *r*, with both indices starting from 0.

The function *c* is a piecewise function defined as follows:

$$c(0,0) = c(n,0) = c(n,n) = 1$$

$c(n,r)=c(n-1,r-1)+c(n-1,r)$ for $0<r<n$

The formula can be thought as a way of composing a triangle-like structure with every element within the external border evaluating to 1 and each internal one composed by adding the elements in above row on the left and on the right:

c(0,0)	1
c(1,0) c(1,1)	1 1
c(2,0) c(2,1) c(2,2)	1 2 1
c(3,0) c(3,1) c(3,2) c(3,3)	1 3 3 1

The entries $c(n,r)$ have a combinatorial interpretation.

Proposition. *Let S be a set with n elements. Then* $c(n,r)$ *is the number of subsets of S with r elements. In other words, the number of combinations of r elements that you can get from a set with n elements.*

Proof. If $r=0$ or $r=n$, then there is only one way to compose the combination.
Let's prove the general case by induction on *n*.
Base case: Let *S* be the set with 1 element. Then the statement is true both when $r=0$ and when $r=1$, since there is only one subset of *S* with 0 elements and 1 subset of *S* with 1 elements.
Inductive step. Assume $n>1$, $1\le r\le n-1$ and that the preposition is true for *n-1*. Let *y* be a fixed element of *S*. Let S_0 be the set of all elements of *S* except y. S_0 is then a set with *n*-1 elements. Divide the collection of all *r*-element subsets of *S* into two piles, one consisting of those containing *y* and the others not containing *y*. The first pile consists of exactly those subsets of *S* obtained by taking an (*r*-1)-elements subset of S_0 and adjoining *y*. By induction applied on S_0 there are exactly $c(n-1,r-1)$ of these. The second pile consists exactly of the *r*-element subsets of S_0 of which there are exactly $c(n-1,r)$. Thus the number of *r*-element subsets of *S* is $c(n,r)=c(n-1,r-1)+c(n-1,r)$.

Lemma. $c(n,r)=\frac{n!}{r!(n-r)!}$

Proof. Induction on *n*. The base case with $n=0$ is trivially true.
Given $n>0$ assume the proposition for *n-1* and for all *r* with $0\le r\le n-1$
Now, $c(n,0)=\frac{n!}{0!n!}=1$ $c(n,n)=\frac{n!}{n!(n-n)!}=1$

For $0<r<n$ we have,

$$c(n,r)=c(n-1,r-1)+c(n-1,r)=\frac{(n-1)!}{(r-1)!(n-r)!}+\frac{(n-1)!}{r!(n-1-r)!}=$$

$$=\frac{(n-1)!}{(r-1)!(n-r-1)!}\cdot\left(\frac{1}{n-r}+\frac{1}{r}\right)=\frac{(n-1)!}{(r-1)!(n-r-1)!}\cdot\frac{n}{(n-r)r}=\frac{n!}{r!(n-r)!}$$

Binomial coefficient notation: $c(n,r)=\binom{n}{r}$

Binomial Theorem. *For every integer* $n\geq 1$

$$(x+y)^n = \binom{n}{0}x^n+\ldots+\binom{n}{r}x^{n-r}y^r+\ldots+\binom{n}{n}y^n = \sum_{r=0:n} x^{n-r}y^r$$

Proof. By induction on *n*.

For *n*=1 the theorem is trivially proved $(x+y)=\binom{1}{0}x+\binom{1}{1}y$

Assume $n>1$ and the theorem true for *n*-1, then

$$(x+y)^n=(x+y)(x+y)^{n-1}=x(x+y)^{n-1}+y(x+y)^{n-1}$$

Using the inductive hypothesis, we get

$$(x+y)^n = \binom{n-1}{0}x^n+\binom{n-1}{1}x^{n-1}y+\ldots+\binom{n-1}{n-1}xy^{n-1}+$$

$$+\binom{n-1}{0}x^{n-1}y+\ldots+\binom{n-1}{n-2}xy^{n-1}+\binom{n-1}{n-1}y^n$$

Thus the coefficient of $x^{n-r}y^r$ for $0<r<n-1$ is

$$\binom{n-1}{r}+\binom{n-1}{r-1}=\binom{n}{r}$$

Since $\binom{n-1}{0}=\binom{n-1}{n-1}=\binom{n}{0}=\binom{n}{n}=1$ we finally have the Binomial Theorem.

Integer representation

Theorem. Let *b* be an integer greater than 1. If *n* is an arbitrary positive integer, it can be uniquely expressed in the form $n = r_k b^k + ... + r_1 b + r_0$ where *k* is a non negative integer and $r_0 \dots r_k$ are non negative integers less than *b* and $r_k \neq 0$. The representation is called the ***base b expansion of n***.

Proof. Suppose all numbers $< n$ can be written in base *b*. To write *n* in base *b*, first divide (using division theorem) *n* by *b* to get $n = bq + r_0$ for unique numbers *q* and r_0 with $0 \leq r_0 < n$. By induction the quotient *q* may be written as $q = r_k b^{k-1} + \dots + r_2 b + r_1$ for unique integers $r_k \dots r_1$. Then, $n = bq + r_0 = b(r_k b^{k-1} + \dots + r_2 b + r_1) + r_0 = r_k b^k + ... + r_1 b + r_0$.

Base conversion. To get *n* in base *b*, first divide *n* by *b*, then successively divide the quotients by *b*.

$$
\begin{aligned}
n &= bq_0 + r_0 \\
q_0 &= bq_1 + r_1 \\
q_1 &= bq_2 + r_2 \\
&\vdots \\
q_{n-2} &= bq_{n-1} + r_{n-1} \\
q_{n-1} &= b0 + r_n
\end{aligned}
$$

The process stops when a quotient with value 0 is reached. The digits are the remainders: $n = (r_n ... r_0)_b$.
The conversion of a number to base 2 can be set up as a special case of *Russian Paesant Arithmetic*.

Given a number *a* the number of words to represent it in base *b* are $\lfloor \log_b a \rfloor + 1$.
E.g. *a=97* and *b=5*. $\lfloor \log_5 97 \rfloor + 1 = 2 + 1 = 3 \rightarrow 97 = 3 \cdot 5^2 + 4 \cdot 5^1 + 2 \cdot 5^0 = (342)_5$

Arithmetic

Let *a* and *b* be two integers represented as $a = (a_n \dots a_0)_w$ and $b = (b_n \dots b_0)_w$ for a given base *w*. We will measure the algorithms complexity in terms of *n*.

Addition

To add *a* and *b* we first add the rightmost words. This gives: $a_0 + b_0 = c_0 \cdot w + s_0$, where s_0 is the rightmost word of the result and c_0 is the carry, which is 0 or 1.

Next we add the next pair of words and the carry: $a_1+b_1+c_0=c_1\cdot w+s_1$, where s_1 is the next word from right of $(a+b)_w$.

The procedure continue while we add a_n, b_n and c_{n-1} to obtain $c_n\cdot w+s_n$. This procedure produces $(s_{n+1}\ldots s_0)_w$ which could be, if $c_n=s_{n+1}\neq 0$, one word greater than the addends.

Complexity. The algorithm cycles *n+1* times. For each iteration there is a fixed number of additions of 3 words. The complexity is thus *O(n)*.

Subtraction

The subtraction works similarly to the addition. Starting from the right-side we subtract the second word from the first. Every time recording if there was a borrow. A borrow will be eventually subtracted from the next iteration result.

Multiplication

A naive approach to multiply *a* and *b* could be to add the first number to the result a number of times equal to *b*. This algorithm *complexity* is $O[(\lfloor \log_w a\rfloor+1)\cdot b]$.

A better approach, uses the distributive law and the binary expansion of *b*.

$$a\cdot b=a\cdot(b_0 2^0+b_1 2^1+\ldots b_n 2^n)=a\,b_0 2^0+a\,b_1 2^1+\ldots a\,b_n 2^n$$

Where $a\,b_i=a$ if $b_i=1$ and $a\,b_i=0$ if $b_i=0$.

Each time we multiply a term by 2, we shift it's binary representation one place to the left and add a zero to the tail of the expansion. Consequently, $a\,b_i 2^i$ is efficiently obtained by shifting the binary representation of $a\,b_i$ *i* places to the left and pad with zeros.

In every iteration we shift the first number on the left by one bit (i.e. we multiply *a* by 2^i) and we add it to the result if $b_i\neq 0$.

Complexity. In the worst case the first number is added $\lfloor \log_2 b\rfloor+1$ times (i.e. every $b_i\neq 0$) and each addition costs $\approx\lfloor \log_w a\rfloor+1$ (we are not considering that *a* is left shifted one bit per iteration). The worst case cost is thus $O[(\lfloor \log_w a\rfloor+1)\cdot(\lfloor \log_2 b\rfloor+1)]$.

Division

The naive algorithm to divide *a* by *b>0*, subtracts *b* from *a* as many times as necessary until what is left is less than *b*. The number of times we perform the subtraction is the quotient *q*, what is left is the remainder *r*. If *a*<0, we find the magnitude using the absolute value of *a* as above, but in the end, since the remainder shall be positive, if $r \neq 0$ we set $q = -(q+1)$ and $r = b - r$, else if $r = 0$ we only set $q = -q$. This algorithm complexity is $O[(\lfloor \log_w a \rfloor + 1) \cdot q]$

A better approach is to use a technique similar to the multiplication. Set $q = 0$ and then find the greatest *i>0* such that $b \cdot 2^i < a$. Add to the quotient *q* the value 2^i and subtract from a the value just added to the quotient. Repeat the process while *a>d.* In the end set the remainder *r=a.*

Complexity. Similar to the improved multiplication method.

More efficient algorithms exist for multiplication and division, for example *Comba*, *Karatsuba* and *Toom-Cook* methods.

Exponentiation

Given a base *b* and an exponent *e*, a naive approach is to repeatedly multiply the base *e* times. The complexity is thus equal to the multiplication complexity times *e*.

A better approach is the so called "*square and multiply*" method. If the exponent *e* is represented in base two as $e = (e_k \ldots e_0)_2$, the operation becomes:

$$b^e = b^{e_k 2^k + \ldots e_0 2^0} = b^{e_k 2^k} \cdot \ldots \cdot b^{e_0 2^0}$$

Starting from $b^{e_0 2^0}$, for every iteration $i \geq 1$, *b* is squared and, if $e_i \neq 0$ it is multiplied to the result.

Complexity. The worst case performs $\log_2 e$ multiplications. The bottleneck here is that the numbers involved in the multiplications quickly become very big. And the multiplication becomes more and more expensive on each iteration.

Modular Exponentiation

First note that $(a \cdot b \cdot c)_m = [(a \cdot b)_m \cdot c]_m$

Thus, given the previously described exponentiation algorithm we can, after each multiplication, immediately find the modulus of the current result, speeding up the computation dramatically.

Divisibility

Divisibility. If *a* and *b* are integers with $a \neq 0$, we say that *a* **divides** *b* if there is an integer *c* such that *b=ac*, or equivalently, if *b/a* is an integer. When *a* divides *b* we say that *a* is a **factor** of *b*. The notation $a|b$ denotes that *a* divides b.

Theorem. *Let a, b, c be integers, where* $a \neq 0$. *Then*

i. if $a|b$ and $a|c$ then $a|(b+c)$
ii. if $a|b$ then $a|bc$ for any integer c (the converse is also true, try with *c=1*).
iii. If $a|b$ and $b|c$ then $a|c$

Proof.

i. $b=as \wedge c=at \rightarrow b+c=a(s+t) \rightarrow a|(b+c)$
ii. $b=as \rightarrow bc=asc \rightarrow a|bc$ for any integer *c*
iii. $b=as \wedge c=bt \rightarrow c=ast \rightarrow a|c$

Corollary. *If* $a|b$ *and* $b|a$ *then* $a=\pm b$
Proof. $b=as \wedge a=bt \rightarrow a=ast \rightarrow st=1 \rightarrow s=t=\pm 1 \rightarrow a=\pm b$

Corollary. *If* $a|b$ *and* $c|d$ *then* $ac|bd$
Proof. $b=as \wedge d=ct \rightarrow bd=acst \rightarrow ac|bd$

Corollary. *If* $ac|bc$ *then* $a|b$
Proof. $bc=act \rightarrow b=at \rightarrow a|b$

<u>*Attention*</u>. *If* $a|bc$ *does not imply that* $a|b$ *or* $a|c$. For example $4|2\cdot 2$ but $4 \nmid 2$

Division Theorem. *Let a be an arbitrary integer and b a non negative integer. Then there are unique integers q and r, with* $0 \leq r < b$, *such that* $a=bq+r$.
Proof. (Existence) Let *L* be the set of non-negative integers of the form $a-bq$, where *q* is an integer. This is nonempty since *-bq* can be made arbitrary big (taking *q* negative). By the *WOP* there is a least element $r=a-bq_0$. Thus *r* is non-negative and $0 \leq r < b$. If $r \geq b$ then $r-b \geq 0$ and consequently we can define $r_1=a-bq_0-b=a-b(q_0+1) \geq 0$ an element of *L* smaller than *r*. That is impossible.

(Uniqueness). Suppose that $a=bq+r$ and $a=bs+t$. Then $r-t=b(s-q)$. Without loss of generality, assume $r\geq t$ so that $0\leq r-t=b(s-q)\leq r<b$. Dividing both sides by b we get $0\leq s-q<1$. Since $s-q$ is an integer, we have that $s-q=0\rightarrow s=q$ and consequently $r-t=0\rightarrow r=t$.

(Existence, induction alt.). Assuming $a\geq 0$. *Base case.* if $a=0$ we set $q=r=0$. *Inductive step.* If $b>a$ we can directly set $q=0$ and $r=a$. If $0<b\leq a$ then $0\leq a-b<a$, thus for inductive hypothesis $a-b=bq_0+r_0$ thus $a=b(q_0+1)+r_0=bq+r$. By induction the existence is confirmed for every $a\in\mathbb{N}$.

In the equality given by the division algorithm, *b* is the **divisor**, *a* is the **dividend**, *q* is the **quotient** and *r* is the **remainder**. With the given definition of divisibility, *b* divides *a* if and only if *r=0*, in such a case *b* is a **factor** of a.

Prime Numbers

Primes. An integer *p* greater than 1 is called **prime** if the only positive factors of *p* are 1 and *p*. A positive integer that is greater than 1 and is not prime is called **composite**.

Lemma[1]. *If p is prime and* $p|a_1\cdots a_n$, *where each* a_i *is an integer, then p divides* a_i *for some* $i\leq n$.
Proof. (by induction) If *n=1* then $p|a_1$ and the lemma is immediately verified. Assume that the lemma is verified for $k\geq 1$. Let's set $A=a_1\cdots a_k$. If $p|(a_1\cdots a_{k+1}=A\,a_{k+1})$ there can be two cases: $(p,A)=1 \rightarrow p|a_{k+1}$ or $(p,A)\neq 1 \rightarrow p|a_1\cdots a_k \rightarrow p|a_i$ for inductive hypothesis.

Theorem (Fundamental Theorem of Arithmetic). *Every integer greater than 1 can be written uniquely as a prime or as the product of two or more primes.*
Proof. (*Existence*) By complete induction. The base step is trivial since 2 is prime. If *n > 2* is prime, then we've finished. Otherwise, *n=ab* with *1<a<n* and *1<b<n*. By hypothesis, $a=p_1\cdots p_r$ and $b=q_1\cdots q_s$ are products of primes. So $n=ab=p_1\cdots p_r q_1\cdots q_s$ that is a product of primes.
(*Uniqueness*) If *n* can be written as product of primes in two different ways $n=p_1\cdots p_s=q_1\cdots q_t$. Then, when we remove all common primes from the two sides we have $p_{i1}\cdots p_{iw}=q_{j1}\cdots q_{jv}$ where no common prime occurs on both sides. By previous lemma, follows that $p_{i1}|q_{jk}$ for some *k*. Because no prime divides another prime, this is impossible.

Proposition. *Every natural number* $n\geq 2$ *is divisible by a prime number.*

1 Proof depends on proposition exposed in the Bezout's identity paragraph: *a*|*bc* and (*a*,*b*)=1 → *a*|*b*

Proof. Base case. $P(2)$ is true, because *2* is prime and divides itself. *Induction step.* Assume $P(k)$ true for all *k* where $2 \le k < m$. If *m* is prime then it is divisible by a prime number, itself. If *m* is not prime then $m = ab$, where $2 \le a < m$ and $2 \le b < m$. Because $2 \le a < m$ then for complete induction hypothesis $P(a)$ holds. Since *a* is divisible by a prime and *a* divides *m* then *m* is divisible by the same prime.

Proof (alt.). For any number $a > 2$, let *L* be the set of numbers ≥ 2 which divide *a*. Since *a* is a positive divisor of itself *L* is nonempty. Thus for the well ordering principle there is *b* in *L* such that it is the least divisor of *a*. If *b* is not prime then *b=ck*, thus there is $c < b$ such that *c* divides *b* and consequently *a*. But that generates a contradiction because *b* is the least divisor of *a*.

Theorem. *If n is a composite integer then has a prime divisor less than or equal to* $\sqrt{n}$.
(*Contrapositive. If an integer n is not divisible by any prime less than or equal to* $\sqrt{n}$ *then is prime)*
Proof. If *n* is composite then it has at least two factors *a* and *b*, with $1 < a < n$ and $1 < b < n$. If both the factors are greater than $\sqrt{n}$ then $n = ab > \sqrt{n}\sqrt{n} = n$. That is impossible.

Trial-division factorization. We divide *n* by all primes not exceeding $\sqrt{n}$ and conclude that *n* is prime if it is not divisible by any of these. The procedure can be iterated to produce the prime factorization of *n*. That is, if a prime factor *p* is found, with $1 < p \le \sqrt{n}$ then we repeat the process to find a factor p_1 for *n/p*, with $p \le p_1 \le \sqrt{n/p}$. Note that *n/p* has no prime factors less than *p,* such numbers were tested by the previous iterations.

Sieve of Eratosthenes.
The algorithm is used to find all primes not exceeding a specified positive integer.
Given the list of integers less than or equal an integer *n*. First the set of all primes not exceeding $\sqrt{n}$ is found. Then for each p_i the algorithm removes all its multiples from the list. All the remaining integers are prime. This follows the fact that, to be composite, a number should have a prime factor not exceeding $\sqrt{n}$.

Theorem (Infinitude of Primes). *There are infinitely many primes.*
Proof. Assume there are finitely many primes $P = \{p_1, \ldots, p_n\}$. Let $q = p_1 \cdots p_n + 1$ then *q* is prime or a product of prime. None of the primes in *P* divides *q* because if $p_i | q$ then $p_i | (q - p_1 \cdots p_n = 1)$ and that is impossible. Hence there is a prime not in the set *P* and this is either *q* or a factor of *q*.

Corollary. *Because there are infinitely many primes, given any positive integer there is always a prime greater than this integer.*

Lucas-Lehmer Test. An efficient test for determining whether $2^p - 1$ is prime.

Divisibility Exponential Notation

Suppose $a = p_1^{e_1} \cdots p_n^{e_n}$ and $b = p_1^{f_1} \cdots p_n^{f_n}$ where $p_1, \ldots, p_n$ include all primes that divide either *a* or *b*, and some of the exponents e_i or f_i may be zero.

Proposition. *With a and b as above, a divides b iff* $e_i \le f_i$ *for all* $i = 1 \ldots n$

Proof. If for all $i = 1, \ldots, n$ we have $e_i \le f_i$, then $c_i = f_i - e_i \ge 0$. Hence defining $q = p_1^{c_1} \cdots p_n^{c_n}$ we have that $b = aq$. Conversely, if *a* divides *b*, then $b = aq$ for some natural number *q*. Then every prime that divides *q* also divides *b*. Write *q* as a product of primes, as above. Then $c_i \ge 0$ and $b = aq$ means that $f_i = e_i + c_i$ for each *i*. Hence $e_i \le f_i$.

Notation: $p^e \| a$ is the power of *p* in the prime factorization of *a*. Thus, $p^e \| a$ if p^e divides *a* but p^{e+1} does not.

Greatest Common Divisor

A **common divisor** of *a* and *b* is an integer *e* such that *e* divides *a* and *e* divides *b*.

A number *d* is the ***greatest common divisor*** (*gcd*) of *a* and *b* if:

i. *d* is a common divisor of *a* and *b;*
ii. *d* is multiple of every other common divisor of *a* and *b* (thus is the greatest).

We denote the *gcd* of *a* and *b* by (a, b).

Proof.

Existence. Consider the set $S = \{ax + by > 0 : \ x, y \in \mathbb{Z}\}$, since the integers *a* and *b* are not both zero, then *S* is not empty, thus for the *WOP* there is a least element $d = as + bt$. Let's prove that $d = (a, b)$. Dividing *a* by *d* we have $a = dq + r$, $0 \le r < d$. Then $r = a - dq = a - (as + bt)q = a(1 - sq) + b(-tq)$.

Thus *r* is of the form *ax+by* as well. If $r > 0$ then $r \in S$ and $r < d$. But this is impossible since *d* is the least element of *S*. Follows that $r = 0$ and $d | a$. In the same way we find that $d | b$ and the first condition for the *gcd* is met. For the second condition, given a common divisor *z* then $z | a$ and $z | b$ that is $a = zk$ and $b = zw$ and thus $d = as + bt = zks + zwt = z(ks + wt)$ and $z | d$ (i.e. *d* is the max divisor).

Uniqueness. If d_1 and d_2 are both *gcd*, then, by *ii* we have that $d_2|d_1$ *and* $d_1|d_2$. *Thus* $d_1=d_2k_2$ and $d_2=d_1k_1$. Follows that $d_1=d_1k_1k_2 \rightarrow k_1k_2=1 \rightarrow k_1=k_2=\pm 1$ and thus that $d_1=\pm d_2$. By convention the *gcd* is positive, thus is unique.

One, inefficient, way to find the *gcd* of two integers *a* and *b* is to first find their prime factorization, then multiply together their common prime factors taken with the minimum exponent.

Two numbers *a* and *b* are ***coprime*** or relatively prime if their *gcd* is 1.

Euclid's Algorithm

Algorithm to find the greatest common multiple of two integers *a* and *b*.

Theorem. *Given two integers a and b, with a>b, if* $d|a$ *and* $d|b$ *then* $d|(a-b)$
Proof. $d|a \rightarrow a=k_1d$ and $d|b \rightarrow b=k_2d$.
Combining the two equations we get $a-b=d(k_1-k_2) \rightarrow d|(a-b)$

We can iterate the theorem application until $a-ib>0$, naturally originating to the following theorem.

Theorem. *Given two integers a and b. If* $d|a$, $d|b$ *and* $a=bq+r$, *with q and r the quotient and the remainder of the integer division respectively, then* $d|(a-bq)$.
Proof. $d|a \rightarrow a=k_1d$ and $d|b \rightarrow d|bq \rightarrow bq=k_2d$ for every q.
Combining the two equations, $a-bq = d(k_1-k_2) \rightarrow d|(a-bq=r)$.

Intuitive way to understand 3|a and 3|b → 3|a-b

a = 3k	----	----	----	k=4
b = 3z	---	---	---	z=3
a-b = 3(k-z)	-	-	-	k-z=1

The algorithm
The algorithm is faithfully based on the above theorem. If *d* is the *gcd* then as it divides both *a* and *b* then it divides their integer division remainder *r.*

Given two natural numbers *a* and *b*, apply the *Division Theorem* successively as follows:

$$b = a\,q_1 + r_1$$
$$a = r_1 q_2 + r_2$$
$$r_1 = r_2 q_3 + r_3$$
$$\vdots$$
$$r_{n-2} = r_{n-1} q_n + r_n$$
$$r_{n-1} = r_n q_{n+1} + 0$$

When we reach the point where r_n divides r_{n-1} with 0 remainder, then r_n is the *gcd* of *a* and *b*. That is $d|r_n \wedge d|0 \rightarrow d = r_n$.

Efficiency of Euclid's Algorithm

Let $N(a,b)$ denote the number of steps needed to obtain the last non-zero remainder of *a* and *b* $(a<b)$ in *Euclid's* Algorithm using division. Thus how quickly the sequence $r_1, r_2, \ldots r_n$ of remainders decreases. A large quotients sequence implies a rapid decrease in the remainders and that implies a small $N(a,b)$.

The worst case is given when *a* and *b* are two consecutive elements of the *Fibonacci's* sequence.

Let $a = F_{n+1}$ and $b = F_n$, because $r = F_{n+1} - F_n = F_{n-1}$, then we have that *r=a-b* and *q=1*. The pattern repeats for all the subsequent steps until the last nonzero remainder, $F_2 = 1$ is not found. Thus we have that $N(F_n, F_{n+1}) = n-2$ (for example: $F_4 - F_3 = F_2 = 1$, then $N(F_3, F_4) = 1$).

Theorem (**Lame's Theorem**). *Let a and b be two natural numbers. Suppose that a<b and* $a<F_n$, *then* $N(a,b) < N(F_n, F_{n+1}) = n-2$.

Proof. Let $b = aq_1 + r_1$, $a = r_1 q_2 + r_2$ with $r_1 < a$ *and* $q_2 \geq 1$ and assume $a < F_n$. By induction.

Base case. $\forall b \in \mathbb{N} \setminus 1$ if $1 < b$ and $1 < F_3$ then $N(1,b) = 0 < N(F_3, F_4) = 1$ is true.

Assuming the theorem true for all *k<n.* If $r_1 < F_{n-1}$ then by induction $N(r_1, a) < N(F_{n-1}, F_n) = n-3$.

If $r_1 \geq F_{n-1}$ then $F_{n-1} + F_{n-2} = F_n > a \geq r_1 + r_2 \geq F_{n-1} + r_2 \rightarrow r_2 < F_{n-2}$. By induction, $N(r_2, r_1) < n-4$. In either case $N(a,b) = N(r_1, a) + 1 = N(r_2, r_1) + 2 < n-2$.

To transform the theorem into a practically usable form, we need to know how many digits the Fibonacci number F_n has.

List of smallest Fibonacci numbers with a given number of digits (base 10):

$F_1=1$ $F_7=13$ $F_{12}=144$ $F_{17}=1597$

Can be proven that every five elements in the sequence the Fibonacci number gains a digit.

Now, if F_{5i+2} has $i+1$ decimal digits, then any number a with d digits satisfies $a<F_{5d+2}$ that has $d+1$ digits. Said that, we have the following important application.

Corollary. *If a < b and a has d digits, then* $N(a,b)<N(F_{5d+2},F_{5d+3})=(5d+2)-2<5d$

Follows that on the worst possible case for the Euclid's algorithm is guaranteed to be less that *5d* steps.

Bezout's Identity

Theorem (Bezout's Identity). *If d the greatest common divisor of a and b, then d=as+bt for some integers s and t.*

Proof. Assuming a and b not both zero and consider the set $L=\{ax+by>0\}$. *Then, since a and b are not both zero, the set is not empty and thus has a minimum value d=as+bt. We'll prove that* $d=(a,b)$.

First we prove that $d|a$ and $d|b$. Let $a=dq+r$, then $r=a-dq=a-(as+bt)q=a(1-sq)+b(-tq)$ is compatible with the L elements definition. If $r>0$ then $r\in L$ but since, by division theorem, $r<d$ that is impossible because d is the least element of L. Follows that $r=0$, and thus d divides a. The same procedure can be followed to prove that d divides b.

Now we prove that every common divisor of a and b also divides d (and thus is less that d). Let z be an arbitrary common divisor of a and b. Then by setting $a=zk$ and $b=zw$, we have that $d=as+bt=zks+zwt=z(ks+wt)$ and thus that z divides d (note that since $z\le d$ $\rightarrow$ only $z=d$ is in L).

Proof (induction via Euclid's algorithm). Intuitively, the *gcd* is first found via *Euclid's* algorithm, then starting from the bottom we replace in each iteration, the quotients and the remainders.

More formally, if a divides b then a is clearly the *gcd* of a and b, and $a=a\cdot 1+b\cdot 0$, so the theorem is true in that case. If a does not divide b the *Euclid's* Algorithm contains at least two divisions. Suppose that it contains $n+1$ divisions ($n\ge 1$) so that r_n is the last nonzero remainder in the algorithm. We prove the theorem by induction on n.

If $n=1$, then *Euclid's Algorithm* for a and b has the form

$$b=aq_1+r_1$$
$$a=r_1q_2+0$$

Then $r_1=(a,b)$ and $r_1=b\cdot 1+a\cdot(-q_1)$, so *Bezout's* identity holds.

Assume the theorem is true for $n=k-1$, so is true for any two numbers whose *Euclid's* algorithm involves k divisions. Suppose *Euclid's* algorithm for a and b involves $k+1$ divisions:

$b = a q_1 + r_1$
$a = r_1 q_2 + r_2$
$r_1 = r_2 q_3 + r_3$:
$r_{k-2} = r_{k-1} q_k + r_k$
$r_{k-1} = r_k q_{k+1} + 0$

Notice that if we omit the first line, what is left is the Euclid's algorithm for a and r_1, that it requires k divisions. So for the induction assumption, r_k is the *gcd* of r_1 and a, with $r_k = au + r_1 v$ for some integers u and v.

Now $b = a q_1 + r_1$, so $(b, a) = (a, r_1) = r_k$. Moreover, substituting $r_1 = b - a q_1$ into the equation $r_k = au + r_1 v$ gives $r_k = au + (b - a q_1) v = bv + a(u - q_1 v)$.

Hence *Bezout's* identity holds for a and b. The theorem is true by induction.

Solving *Bezout's* identity by *Euclid's* algorithm is often called the **Extended Euclidean Algorithm** (EEA).

It is easier to do the computations by starting at the top of *Euclid's* Algorithm, rather than the bottom, and successively write the original two numbers and all the remainders as linear combinations of the two original numbers.

The process can be done easily by setting up a matrix of three columns: remainders, coefficients of a and coefficients of b. We call this matrix the *EEA* matrix.

Example: $e = 365x + 1876y$

e	*x*	*y*
1876	0	1
365	1	0
365·5	5	0
51=1876-365·5	-5	1
51·7	-35	7
8=365-51·7	36	-7
8·6	216	-42
3=51-8·6	-221	43
3·2	-422	86
2=8-3·2	430	-93
1=3-2	-651	136

Thus we've finally found that $1 = 365(-651) + 1876(136)$

Corollary. *Two numbers a and b are **coprime** iff there are integers s and t such that 1=as+bt.*

Proof. If $(a,b)=1$ then for the *Bezout's* identity there are integers *s* and *t* such that *1=as+bt*. Conversely, if *1=as+bt* for some integers *s* and t. If *d* is the *gcd* then it divides both *a* and *b*, then *d* divides *as+bt=1*, so *d=1* or *-1*. The *gcd* of *a* and *b* is positive thus *d=1* and *a* and *b* are coprime.

Corollary. *If e divides a and b then e divides (a,b).*
Proof. d=(a,b) $\rightarrow$ *d=ar+bs* for some integers *r* and *s*. If *e* divides *a* and *b* then *a=ef* and *b=eg* for some integers *f* and *g*. Then *d=efr+egs = e(fr+gs)*. So *e* divides *d*.

Corollary. *If a divides bc, and a and b are coprime, then a divides c.*
Proof. 1=ar+bs for some integers *r* and *s*. Multiply both sides by *c* to get *c=arc+bsc*. Now, *a* obviously divides *acr*. If *a* divides *bc* then it divides *bsc*. Thus *a* divides their sum *c*.

Proposition. *For every integers a,b,m:*

i. (ab,m) *divides* $(a,m)(b,m)$

ii. If a and b are coprime, then $(ab,m)=(a,m)(b,m)$

Proof. Let *(a,m)=ra+sm, (b,m)=tb+vm.* Then *(a,m)(b,m)=ratb+ravm+smtb+smvm = abrt+mz.*
Since *(ab,m)* divides *ab* and *m, therefore (ab,m)* divides *abrt+mz=(a,m)(b,m).*
For the second part notice that

$(a,m)=aX+mY$ and $(ab,m)=abU+mW$

$((a,m)|a \rightarrow (a,m)|ab)$ and $(a,m)|m \rightarrow (a,m)|(abU+mW) \rightarrow (a,m)|(ab,m)$

Then we can write $(ab,m)=(a,m)e$ for some integer *e*.
Following the same reasoning also $(b,m)|(ab,m)$.
Since *a* and *b* are coprime also (a,m) and (b,m) are coprime. Thus, for the previous corollary, follows that (b,m) divides *e.* Thus $(ab,m)=(a,m)(b,m)k$ *f*or some intege*r k.* Since (ab,m) divides $(a,m)(b,m)$, we must have *k=1.*

The previous proposition is useful for factoring large numbers.

Linear Diophantine Equations

For numbers *a, b, e, Bezout's* Identity can be conveniently used to decide if there are integers solutions to the equations of the form *ax+by=e*. And to find the solution if there is one.

Proposition. *Given integers a, b, e, there are integers x and y with ax+by=e iff d=(a,b) divides e.*
Proof. If *ax+by=e*, then the gcd divisor of *a* and *b* divides the sum of their multiples, and thus *e*.
If *d* divides *e* then *e=dk* for some integer *k*. For *Bezout's* Identity we can find integers *r,s* so that *d=ar+bs*. Multiplying both sides by *k* we get *e=dk=ark+bsk=ax+by.*

The proof also shows how to find a solution of *ax+by=e* given that $(a,b)|e$.
As an optimization, if we use the *EEA* matrix to find (a,b) we can stop the procedure as soon as we find a remainder *c* that divides *e*.

General solution. To find the general solution of *ax+by=c* we need to find an arbitrary solution of *ax+by=c* then add to it the general solution of the homogeneous equation *ax+by=0.*

Proposition. *Let* $d=(a,b)$. *The general solution of ax+by=0 is* $x=\frac{b}{d}k$ *and* $y=-\frac{a}{d}k$ *for any integer k.*
Proof. Suppose *ax+by=0*. Divide both sides by *d* to get $\frac{a}{d}x=-\frac{b}{d}y$. Since the integers $\frac{a}{d}$ and $\frac{b}{d}$ are coprime, then $\frac{a}{d}$ divides *y* and $y=\frac{a}{d}k$ for some integer *k*. Finally $\frac{a}{d}x=-\frac{b}{d}\frac{a}{d}k$ that gives $x=-\frac{b}{d}k$.

Corollary. *If* x_0, y_0 *is a solution of ax+by=c, then the general solution ax+by=c is of the form* $x=x_0+\frac{b}{d}k$ *and* $y=y_0-\frac{a}{d}k$.

Least Common Multiple

Given two natural numbers *a* and *b*, a number *m>0* is a **common multiple** of *a* and *b* if *m=ar=bs* for two natural numbers *r* and *s*. There are infinitely many common multiples and the **least common multiple** is the smallest in this set and is usually denoted as $lcm(a,b)$ or $[a,b]$.

Proposition. *Any two numbers a and b have a least common multiple.*
Proof. Since the set *L* of common multiples of *a* and *b* contains their product $a\cdot b$, then *L* is not empty and thus for the *WOP* has a least element, which is the least common multiple.

Proposition.

i. *The lcm of a and b is the product ab divided by the gcd:* $[a,b]=ab/(a,b)$
ii. *The lcm of a and b divides every common multiple of a and b.*

Proof. Assuming that $d=(a,b)$, we consider two separated cases: *d=1* and d>1.

If *d=1*. Clearly *ab* is a common multiple of *a* and *b, w*e must prove that it is the least. Suppose *m>0* is a common multiple of *a* and *b*. Then *m=as* for some number *s>0* and $b|(m=as)$. Since $(a,b)=1$ then $b|s$, so *s=bt* for some integer *t>0*. Thus *m=as=abt.* Since *t>0* then $m\geq ab$ and *m* is a multiple of *ab*. Thus *ab* is the *lcm* and *ab* divides any other common multiple.

If *d>1*. Let $a=dx$ and $b=dy$, follows that $ab/d=xyd=ay=bx$, so *ab/d* is a common multiple of both *a* and *b*. We have to show that any common multiple of *a* and *b* is a common multiple of *ab/d* (and consequently is the least). Suppose *m>0* is a common multiple of *a* and *b*. Then *m* is a multiple of *d*, so write *m=dk* for some number *k*. Since *(a=dx)|(m=dk) then x|k* and, in similarly, *y|k*. Now for the *Bezout's* identity *d=ar+bs* then *1=xr+ys and thus (x,y)=1*. By the first part of the proof then, *xy* divides any multiple of *x* and *y*, thus *xy|k*. But then *(xyd=ab/d)|(kd=m),* that is *ab/d* divides any common multiple of *a* and *b*.

Congruence

Two integers *a* and *b* are congruent modulo *m*, written $a\equiv b(\mathrm{mod}\, m)$, if $m|(a-b)$ or, equivalently, if *b=a+mk* for an arbitrary integer *k*.

The set of integers to which the integer *a* is congruent modulo *m* is $\{a+mk:\forall k\in\mathbb{Z}\}$.

The division theorem asserts that *a=mq+r,* for two unique integers *q* and *r* with $0\leq r<m$. In terms of congruence, this last equation says that $a\equiv r(\mathrm{mod}\, m)$ and *r* is called the **least non-negative residue** of $a(\mathrm{mod}\, m)$, often simply denoted as "*a mod m*"**.**

Proposition. *Let m be a natural number. Every integer is congruent modulo m to exactly one number in the set* $\{0,\ldots,m-1\}$.

Proof. For the Division Theorem $a=mq+r$ for two unique integers *q* and *r*, such that $0\leq r<m$. Follows that $a-r=mq$ and thus $a\equiv r(\mathrm{mod}\, m)$.

Proposition. *Given m successive integers* $a,\ldots,a+(m-1)$ *and another integer A. Then one and only one of these integers will be congruent to A modulo m.*

Proof. Because $a \equiv r \pmod{m}$ for a unique r such that $0 \le r < m$. Then $a, a+1, \ldots, a+(m-1)$ are congruent to $r, r+1, \ldots, r+(m-1) = r-1$. Now, because $A \bmod m \in \{0, \ldots, m-1\}$, the result follows.

Proposition. *Let a and b be two integers. Suppose the remainder on dividing a by m is r and the remainder on dividing b by m is s. Then* $a \equiv b \pmod{m}$ *iff r=s.*

Proof. For the Division Theorem $a=mq+r$ and $b=mt+s$ for some natural numbers q and t. If $r = s$, then $a - mq = b - mt$, $a - b = m(q-t)$, and so $a \equiv b \pmod{m}$. Conversely, if $a \equiv b \pmod{m}$, then $b = a + mk$ for some k, so if $a = mq + r$ is the result of dividing a by m, then $b = a + mk = mk + mq + r = m(k+q) + r$. Since $0 \le r < m$, this expression for b is what is obtained from the Division Theorem when b is divided by m. By the uniqueness of the quotient and remainder, $s = r$.

In other words, two numbers are congruent modulo *m iff* their least non-negative residues are equal.

Proposition. *Congruence modulo m is an equivalence relation.*

Proof.

i. *Reflexive.* If $a \equiv a \pmod{m}$, then $a=a+mk$, and that is trivially true for $m=0$.

ii. *Symmetric.* If $a \equiv b \pmod{m}$, then $a=b+mk$ and $b=a+m(-k)$. Thus $b \equiv a \pmod{m}$.

iii. *Transitive.* If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$ then $a=b+sm$ and $b=c+tm$. Substituting we get $a = c + (t+s)m$ so $a \equiv c \pmod{m}$.

Proposition. *For all integers a, b, c, d and m*

i. if $a \equiv b \pmod{m}$ then $ka \equiv kb \pmod{m}$

ii. if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ then:

   a) $a + c \equiv b + d \pmod{m}$

   b) $ac \equiv bd \pmod{m}$

Proof.

i. $a = b + ms \rightarrow ka = kb + kms \rightarrow ka \equiv kb \pmod{m}$ (… and also $ka \equiv kb \pmod{km}$)

ii. a) $a = b + ms \wedge c = d + mt \rightarrow a + c = (b+d) + m(s+t) \rightarrow a + c \equiv b + d \pmod{m}$

   b) $a = b + ms \wedge c = d + mt \rightarrow ac = bd + mZ \rightarrow ac \equiv bd \pmod{m}$

Similar properties were found in the "*divides*" relation, with the exception of *ii.a*

If $a|b$ then $ak|bk$

If $a|b$ and $c|d$ then $ac|bd$, but that doesn't imply $(a+c)|(b+d)$

The **cancellation property,** i.e. the converse of proposition *i*, does not necessarily hold. Thus, if $ac \equiv bc \pmod{m}$, then the congruence $a \equiv b \pmod{m}$ does not necessarily follow.
Example: $2 \cdot 3 \equiv 2 \cdot 1 \pmod{4}$ but $3 \equiv 1 \pmod{4}$ is not true.

Proposition. *If* $ac \equiv bc \pmod{m}$ *then* $a \equiv b \pmod{\frac{m}{(c,m)}}$

Proof. Given $d = (c,m)$ and $ac \equiv bc \pmod{m} \rightarrow c(a-b) = mk \rightarrow \frac{c}{d}(a-b) = \frac{m}{d}k$.

Because $(\frac{c}{d}, \frac{m}{d}) = 1$ then $\frac{m}{d} | a-b$ and thus $a \equiv b \pmod{\frac{m}{(c,m)}}$

Corollary. *If* $ac \equiv bc \pmod{mc}$ *then* $a \equiv b \pmod{m}$
*Proof***.** Immediately follows the previous proposition.

Corollary. *The cancellation property holds iff* $(c,m) = 1$
Proof. If the cancellation property holds then $ac \equiv bc \pmod{m} \rightarrow a \equiv b \pmod{m}$ and, because of the previous proposition, (c,m) should be 1. Conversely, if $(c,m) = 1$ the result follows immediately from the previous proposition.

Proposition. *If* $a \equiv b \pmod{m}$ *and* $d | m$ *then* $a \equiv b \pmod{d}$
Proof. $m | (a-b)$ and $d | m \rightarrow d | (a-b)$

Proposition. *For all natural numbers e and integers a, b: if* $a \equiv b \pmod{m}$ *then* $a^e \equiv b^e \pmod{m}$
Proof. The result is a simple induction argument based on $a \equiv b \pmod{m} \rightarrow aa \equiv bb \pmod{m}$

This last proposition can be used to simplify the exponential computations modulo *m.*
Example. If $e = st$ then to compute $a^e \equiv b^e \pmod{m}$ we can first compute $a^s \bmod m = r$. Now, since $a^s \equiv r \pmod{m}$ then $a^e = (a^s)^t \equiv r^t \pmod{m}$.
For convenience, keep the absolute value of the modulus operation result *k* as close to zero as possible.

Proposition. *If* $a \equiv b \pmod{r}$ *and* $a \equiv b \pmod{s}$ *then* $a \equiv b \bmod([r,s])$
Proof. The *lcm* $[r,s]$ divides every common multiple of *r* and *s*. Since $r | a-b$ and $s | a-b$ then $a-b$ is a multiple of both *r* and *s* and thus $[r,s] | (a-b)$.

Congruence relations can help explain some of the well known divisibility tricks by 3, 9, 2, 5, 11, 7, 13.

For example, given an arbitrary integer *a*, we rewrite the number in base 10 expanded form

$$a = a_n 10^n + \ldots + a_0 10^0$$

Since $10 \equiv 1 \pmod 9$ then $10^e \equiv 1 \pmod 9$ for any number *e*. Follows that $a \equiv (a_n + \ldots + a_0) \pmod 9$ and thus that $9 | a$ *iff* $(a_n + \ldots + a_0) \equiv 0 \pmod 9$.

Also since $10 \equiv 1 \pmod 9$ and $3 | 9$ then $10 \equiv 1 \pmod 3$ and thus $3 | a$ *iff* $(a_n + \ldots + a_0) \equiv 0 \pmod 3$.

Divisibility by 2 is trivially proved by noting that $10 \equiv 0 \pmod 2$. Thus $2 | a$ *iff* $2 | a_0$. An identical argument is used to prove divisibility by 5.

Divisibility by 7 is proved by noting that $1001 \equiv 0 \pmod 7$, and thus $1000 \equiv -1 \pmod 7$. By rewriting *a* in base 1000 expanded form $a = a_n 1000^n + \ldots + a_0 1000^0$ we have that a is equivalent to $a_0 - a_1 + a_2 - a_3 + \ldots + (-1)^n a_n$, thus $7 | a$ *iff* such a sum is congruent to 0 modulo 7. An identical argument is used to prove divisibility by 11 and 13.

Linear congruences

We want to solve: $ax \equiv b \pmod m$.

To solve the problem, we need to find two integers *x* and *y* so that $b = ax + my$.

Proposition. *The linear congruence* $ax \equiv b \pmod m$ *has a solution iff* $(a, m) | b$

Proof. Setting $d = (a, b)$. If *d* does not divide *b* then there are no integers *x* and *y* with *ax+my=b*, and so the linear congruence has no solution. If *d* divides *b* then *b=dk* and we can solve the congruence using the *Bezout* identity: $d = as + mt \rightarrow b = ask + mtk \rightarrow b = ax + by$ with *x=sk* and *y=tk*.

To systematically arrive to the solution, we can set up an *EEA* matrix to find $d = (a, m)$ and then multiply it by *b/d* to get the solution. We can simplify the *EEA* algorithm by stopping as soon as we find a divisor of *b* (not necessary to arrive to (*a,m*)) and by computing only the *x* coefficients of the linear diophantine equation.

Proposition. *If* $(a, m) = 1$ *then* $ax \equiv 1 \pmod m$ *has a unique solution modulo m.*

Proof. (*Existence*) The congruence $ax \equiv 1 \pmod m$ is equivalent to the equation *ax+my=1*. If $(a, m) = 1$, then by Bezout's Identity there are integers *s, t* such that *1=as+mt*, and so *x=s* and *y=t* is a solution of the congruence. (*Uniqueness*) If also $aw \equiv 1 \pmod m$ then $a(x - w) \equiv 0 \pmod m$ and so $m | a(x - w)$. Since $(a, m) = 1$, $m | (x - w)$ and $x \equiv w \pmod m$.

Multiplicative Inverse. The solution x of $ax \equiv 1 \pmod{m}$ is the *inverse* of a modulo m.

Corollary. *If (a,m)=1 then* $ax \equiv b \pmod{m}$ *has a solution for all b.*
Proof. Find the inverse a^{-1} of a modulo m and set $x = a^{-1}b$

Proposition. *Given* $ac \equiv bc \pmod{m}$, *the cancellation property holds iff there exists the inverse of c modulo m.*
Proof. If there exists c^{-1} then $acc^{-1} \equiv bcc^{-1} \pmod{m}$ and $a \equiv b \pmod{m}$. If the cancellation property holds then $(c, m) = 1 \rightarrow 1 = cs + mt \rightarrow 1 \equiv cs \pmod{m}$ and $s = c^{-1}$.

General solution. Just like with linear diophantine equations, to find the general solution of $ax \equiv b \pmod{m}$, we need to find an arbitrary solution, then add to it the general solution of the homogeneous congruence $ax \equiv 0 \pmod{m}$.

Then x is a solution of the homogeneous congruence *iff* $m \mid ax$ *iff* $\frac{m}{d} \mid \frac{a}{d}x$ where $d = (a, m)$. Since $(\frac{m}{d}, \frac{a}{d}) = 1$ the last statement is equivalent to $\frac{m}{d} \mid x$, hence $x = \frac{m}{d}k$ for some integer(s) k.

Thus, modulo m, we have $d = (a, m)$ different solutions to the homogeneous congruence, namely:

$x = \frac{m}{d}k$ *for* $k = 0, \ldots d-1$.

Congruence classes

The idea is to use congruence modulo *m* to split the set of integers into a finite collection of disjoint subsets on which we can do arithmetic. We've already proved that the congruence modulo *m* is an **equivalence relation**. When a set *S* has an equivalence relation on it, then the relation **partitions** the set *S* into subsets, called **equivalence classes**, defined by the property that two elements are in the same equivalence class if they are equivalent.

The equivalence class of the integer *a* is called the congruence class of *a* modulo *m,* written $[a]_m$.

$$[a]_m=\{a+mk:\ \forall\ k\in\mathbb{Z}\}$$

The set of all the congruence classes modulo *m* is denoted as $\mathbb{Z}/m\mathbb{Z}$.

The set $\mathbb{Z}/m\mathbb{Z}$ is composed by *m* congruence classes each one containing infinite elements.

$$\mathbb{Z}/m\mathbb{Z}=\{[0]_m,[1]_m,[2]_m,\ldots,[m-1]_m\}$$

Proposition. *For* $a,b\in\mathbb{Z}$, $a\equiv b\pmod m$ *iff* $[a]_m=[b]_m$.

Proof. If $[a]_m=[b]_m$, since $a\in[a]_m$, then $a\in[b]_m$, so $a=b+mk$ for some k or, equivalently, $a\equiv b\pmod m$. Conversely, if $a\equiv b\pmod m$, given an arbitrary integer $d\in[a]_m$ then by definition $d\equiv a\pmod m$ and (by transitivity) $d\equiv b\pmod m$, thus $d\in[b]_m$. Since $d\in[a]_m$ implies $d\in[b]_m$ then $[a]_m\subseteq[b]_m$. A similar argument shows that $[b]_m\subseteq[a]_m$. Thus we have $[a]_m=[b]_m$.

Corollary. *Suppose* $[a]_m$ *and* $[b]_m$ *are two congruence classes and* $c\in\mathbb{Z}$ *is in both* $[a]_m$ *and* $[b]_m$, *then* $[a]_m=[b]_m$.

Proof. If $c\in[a]_m$ then $c\equiv a\pmod m$, so by the previous proposition $[c]_m=[a]_m$. If $c\in[b]_m$, then $c\equiv b\pmod m$, so $[c]_m=[b]_m$. Hence $[a]_m=[b]_m$.

An element of a congruence class modulo *m* is called a **representative** of that class. We may label a congruence class by any representative. Is often convenient to label the class with the least non negative element of the class, but this is not always the case.

Arithmetic on $\mathbb{Z}/m\mathbb{Z}$

$$[a]_m+[b]_m=[a+b]_m$$
$$[a]_m\cdot[b]_m=[a\cdot b]_m$$
$$-[a]_m=[-a]_m$$

For example, this means that the sum a representative of $[a]_m$ and a representative of $[b]_m$ gives a representative of $[a+b]_m$ (not always the least non negative one).
Example. $[7]_{10}+[8]_{10}=[15]_{10}=[5]_{10}$

Theorem. *Addition and multiplication in $\mathbb{Z}/m\mathbb{Z}$ are well defined.*
Proof. We must show that if $[a]_m=[a']_m$ and $[b]_m=[b']_m$ then

$[a+b]_m=[a'+b']_m$
$[a\cdot b]_m=[a'\cdot b']_m$
$[-a]_m=[-a']_m$

To easily prove the statements, we translate them into congruence notation, that we know they are true. If $a\equiv a'(mod\, m)$ and $b\equiv b'(mod\, m)$ then

$a+b\equiv a'+b'(mod\, m)$
$a\cdot b\equiv a'\cdot b'(mod\, m)$
$-a\equiv -a'(mod\, m)$

The congruence classes $[0]_m$ and $[1]_m$ are special, in that

$[0]_m+[b]_m=[b]_m$ ($[0]_m$ is the addition neutral element)
$[1]_m\cdot[b]_m=[b]_m$ ($[1]_m$ is the product neutral element)
$[0]_m\cdot[b]_m=[0]_m$

Given integers *a*, *b* and a natural number $m>1$, all of these notations are equivalent:

$a=b+mk$
$m|(b-a)$
$a\equiv b(mod\, b)$
$[a]_m=[b]_m$

The set of congruence classes modulo *m* is a set on which we can do arithmetic in a natural manner.

Complete sets of representatives

Definition. A **complete set of representatives** for $\mathbb{Z}/m\mathbb{Z}$ is a set of *m* integers $\{r_1,\ldots,r_m\}$ so that every integer in $\mathbb{Z}$ is congruent modulo *m* to exactly one of the numbers in the set. Then the set of all the congruence classes modulo *m* is

$\mathbb{Z}/m\mathbb{Z}=\{[r_1]_m,\ldots,[r_m]_m\}$

We've already proved that given an arbitrary integer this is congruent to one and only one congruence class in the set. Every set of *m* consecutive integers is a complete set of representatives.

Proposition. *Every set of m consecutive integers is a complete set of representatives for* $\mathbb{Z}/m\mathbb{Z}$.
Proof. Given *m* successive integers defined as $a_i=a_1+k$ *for* $0\le k<m$. If they are not a complete set of representatives then there are two elements a_i and a_j such that $[a_i]=[a_1+i]=[a_1+j]=[a_j]$ for $i\neq j$ and $0\le i,j<m$. From the previous equation follows that $[i]=[j]$, but we know that should be $[i]\neq[j]$. The contradiction suggests that the *m* consecutive elements are a complete set of representatives.

Proposition. *If* $\{a_1,\ldots,a_m\}$ *is a complete set of representatives modulo m, then for any integer b,* $\{a_1+b,\ldots,a_m+b\}$ *is a complete set of representatives.*
Proof. If not, then $[a_i+b]=[a_j+b]$ and then $[a_i]=[a_j]$, contradicting the hypothesis.

Proposition. *If* $\{a_1,\ldots,a_m\}$ *is a complete set of representatives modulo m, then* $\{b\,a_1,\ldots,b\,a_m\}$ *is a complete set of representatives modulo m iff* $gcd(b,m)=1$.
Proof. If $gcd(b,m)=1$ and $[a_i b]=[a_j b]$ then there exist the inverse of *b* modulo *m* such that $[a_i]=[a_j]$, contradicting the hypothesis.

Primitive Root Theorem. If *p is a prime number then there exists some integer r so that* $\{0,r,r^2,r^{3,}\ldots,r^{p-1}\}$ *is a complete set of representatives for* $\mathbb{Z}/p\mathbb{Z}$.

In other words, for every representative *a* of $\mathbb{Z}/p\mathbb{Z}$ there is an integer *k* such that $r^k\equiv a(mod\ p)$. Such *k* is called the index or **discrete logarithm** of *a* to the base *r* modulo *p* ($\log_r a=k$).
An integer *r* satisfying the *PRT* is called a **primitive root** modulo *p*.

When we represent the non-zero congruence classes modulo *p* by the powers of a primitive root *r*, then multiplication of congruence classes turns into addition of exponents modulo *p*. That is, if $[r^x]_p=[a]_p$ and $[r^y]_p=[b]_p$ then $[a]_p[b]_p=[r^x]_p[r^y]_p=[r^{x+y}]_p$

Proposition. *Given a set* $R=\{r_1,\ldots,r_m\}$ *of m integers, the following conditions are equivalent:*

i. For every i, j with $1\le i<j\le m$, r_i *is not congruent* r_j *modulo m*
ii. Every integer is congruent modulo m to some $r_i\in R$

A complete set of representatives mod m is a set of integers R satisfying either i or ii.

Proof. Given a set $R=\{r_1,\ldots,r_m\}$ of m integers, the map $r\to[r]_m$ defines a function f from R to $\mathbb{Z}/m\mathbb{Z}$. Then *i* says that f is one-to-one and *ii* says that f is onto[2]. Let $f(R)=\{f(r)\colon r\in R\}$ be the image of the function *f*. Now if $|R|=m$, $|f(R)|$ and $|\mathbb{Z}/m\mathbb{Z}|=m$ denote the cardinalities of the sets *R*, $f(R)$ and $\mathbb{Z}/m\mathbb{Z}$ respectively, then $m=|R|\geq|f(R)|\leq|\mathbb{Z}/m\mathbb{Z}_m|=m$. Also f is one-to-one if $|R|=|f(R)|$, and f is onto if $|f(R)|=|\mathbb{Z}/m\mathbb{Z}|$. Since $|R|=m=|\mathbb{Z}/m\mathbb{Z}|$, it follows that $|R|=|f(R)|$ *iff* $|f(R)|=|\mathbb{Z}/m\mathbb{Z}|$, that is, f is one-to-one *iff* f is onto. So *i* and *ii* are equivalent.

Units

Given a number *a* if there is a number *b* so that $ab=ba=1$ then we call *a* a **unit** and *b* the **inverse** of *a*.

Proposition. *If the inverse of a number exists, then is unique.*

Proof. If *b* and *c* are both inverses of *a*, then *ab=ac=1*. By multiplying both sides by *b* we have $b(ab)=b(ac)\to(ba)b=(ba)c\to b=c$.

In $\mathbb{Z}$ only 1 and -1 have multiplicative inverse, themselves respectively.
In $\mathbb{Q}$ every number, except 0, has a multiplicative inverse.

Proposition. $[1]_m$ *is the only multiplicative identity in* $\mathbb{Z}/m\mathbb{Z}$.

Proof. If we assume that $[e]_m$ is a another multiplicative identity, then given an arbitrary congruence class $[a]_m$, $[e]_m\cdot[a]_m=[a]_m$. In particular $[e]_m\cdot[1]_m=[1]_m$. But since $[1]_m$ is a multiplicative identity as well, $[e]_m\cdot[1]_m=[e]_m$. Thus $[1]_m=[e]_m$.

The trivial, and inefficient, way to find units in $\mathbb{Z}/m\mathbb{Z}$ is to write the whole multiplication table.

Theorem. *In* $\mathbb{Z}/m\mathbb{Z}$ $[a]_m$ *is a unit iff a and m are coprime.*

Proof. If $(a,m)=1$ then by *Bezout's* identity there are integers *r* and *s* such that $1=ar+ms$. Then $[ar+ms]_m=[1]_m$. But $[ar+ms]_m=[ar]_m=[a]_m[r]_m=[1]_m$ so $[r]_m$ is the inverse of $[a]_m$ in $\mathbb{Z}/m\mathbb{Z}$.
Conversely if $[a]_m$ is a unit then there is $[r]_m$ such that $[a]_m[r]_m=[1]_m$. Passing to congruence notation this is equivalent to $ar\equiv1(mod\,m)$, so there is an integer *s* such that $ar+ms=1$, which implies that $(a,m)=1$.

2 If both the domain and codomain have the same number of elements then a function is one-to-one *iff* is onto.

Corollary. *The number of units in* $\mathbb{Z}/m\mathbb{Z}$ *is equal to the number of integers a with* $1 \le a \le m$ *that are coprime to m.*

Proposition. *If* $[a]$ *and* $[b]$ *are units then* $[ab]$ *is a unit.*
Proof. There are $[r]$ and $[s]$ such that $[a][r]=[1]$ and $[b][s]=[1]$ then $[ab][rs]=[1]$.

So the set of units U_m is then closed under the multiplication operation.
Note that U_m can be not closed under the addition operation. That is, the addition of two units can produce a result that is not a unit.

Proposition. *If r is a* ***primitive root*** *modulo p then* $[r]$ *is a unit.*
Proof. Since there must be some power *k,* with *0<k<p,* such that $[1]=[r^k]$ then $[r]$ is a unit and its inverse is $[r^{k-1}]$. Also note that any power *s* of the primitive root is a unit as well: since $[1]=[r^k]$, then if $s \le k$ the inverse is $[r^{k-s}]$ else the inverse is $[r^{p-s+k}]$.

Note that if k=1,then $[r^1]=[1] \rightarrow [r][r^0]=[r][1]=[1]$ and follows that $[r]$ is its own inverse.

Follows that the converse of the Primitive Root theorem holds.

Theorem (PRT converse). *If in* $\mathbb{Z}/p\mathbb{Z}$ *there is a primitive root r then p is a prime number*.
Proof. Every congruence class, other that $[0]$ is of the form $[r^k]$ for some *k*, hence is a unit of $\mathbb{Z}/p\mathbb{Z}$. Because a unit should be coprime to *p* and every r^k is congruent to some number *n*, with $0 \le n < p$, then every number *n<p* is coprime to *p*. Follows that *p* should be prime.

Euler's totient

Euler's phi function (totient). For each $m \ge 1$, $\phi(m)$ denotes the number of integers *a* with $1 \le a \le m$ that are coprime to *m*. The totient $\phi(m)$ is thus equal to the number of units in $\mathbb{Z}/m\mathbb{Z}$.

Proposition. *Given two integers m and n. If* $gcd(m,n)=1$, *then* $\phi(mn)=\phi(m)\phi(n)$.
Proof. Build a matrix of the numbers 1 to *mn* with *m* rows and *n* columns.

1	*1+m*	*1+2m*	*…*	*1+(j-1)m*	*…*	*1+(n-1)m*

2	*2+m*	*2+2m*	*...*	*2+(j-1)m*	*...*	*2+(n-1)m*
3	*3+m*	*3+2m*	*...*	*3+(j-1)m*	*...*	*3+(n-1)m*
⋮	⋮	⋮				⋮
i	*i+m*	*i+2m*	*...*	*i+(j-1)m*	*...*	*i+(n-1)m*
⋮	⋮	⋮				⋮
m	*m+m*	*m+2m*	*...*	*m+(j-1)m*	*...*	*m+(n-1)m*

The numbers in the *i*-th row are of the form $i+km$ as *k* runs from *0* to *n-1*. Let $d=gcd(i,m)$.

If *d>1* then no number in the *i*-th row of the table is relatively prime to *mn*, since if $d|i$ and $d|m$ then $d|(i+km)$ for all *k*. Thus $(mn,i+km)$ is at least d>1. So to count the residues relatively prime to *mn* we need to look at the rows indexed by values of *i* such that $(i,m)=1$, and there are exactly $\phi(m)$ of them.

If *d*=1 then every entry in the *i*-th row is relatively prime to *m*, since $(i+km,m)=1$ by the Euclid's algorithm. Because $\{0,\ldots,(n-1)\}$ is a complete set of representatives modulo *n*, then follows that the entries in the *i*-th row form a complete set of representatives modulo *n (mul* by *m, with (n,m)=1, and add i)*[3]. Thus exactly $\phi(n)$ of them will be relatively prime to *n*, and thus relatively prime to *mn*.

Proposition. *Given a prime number p, and a natural number n.*

$$\phi(p^n)=p^n-p^{n-1}=p^{n-1}(p-1)=p^n(1-1/p)$$

Proof. Create a list of the numbers from 1 to p^n and count how many numbers in the list are not relatively prime to p^n. Because *p* is prime we indeed are counting the multiples of *p* that are less than p^n. There are p^{n-1} of such multiples and they are: $p, 2p, 3p, \ldots, p^{n-1}p$. Thus among the p^n numbers there are $p^n - p^{n-1}$ numbers relatively prime to p^n.

Theorem $\phi(m)=m\cdot\prod_{p_i}(1-\frac{1}{p_i})$, $p_i|m$.

Proof. The fundamental theorem of arithmetic states that if n>1 there is a unique expression for $n=p_1^{k_1}\cdot p_2^{k_2}\cdot\ldots\cdot p_r^{k_r}$ where $p_1<p_2<\ldots<p_r$ are prime numbers and each $k_i>0$.

Repeatedly using the multiplicative property of ϕ and the formula for $\phi(p^k)$ gives

$$\phi(m)=\phi(p_1^{k_1}\cdot\ldots\cdot p_r^{k_r})=\phi(p_1^{k_1})\cdot\ldots\cdot\phi(p_r^{k_r})=p_1^{k_1}(1-1/p_1)\cdot\ldots\cdot p_r^{k_r}(1-1/p_r)=$$
$$=p_1^{k_1}\cdot\ldots\cdot p_r^{k_r}\cdot(1-1/p_1)\cdot\ldots\cdot(1-1/p_r)=m\cdot\prod_{p_i}(1-\frac{1}{p_i})$$

3 Refer to "complete set of representatives" propositions.

Equations

The main application of inverses is equation solving.
If we can find the inverse $[b]_m$ of $[a]_m$ in $\mathbb{Z}/m\mathbb{Z}$ then we can solve $[a]_m X=[c]_m$ for any c simply by setting $X=[b]_m[c]_m=[bc]_m$.

In $\mathbb{Z}/m\mathbb{Z}$ equations can have a solution even when the X coefficient $[a]_m$ is not a unit.
Example. $[6]_{16}X=[14]_{16}$. Even if $[6]_{16}$ is not a unit, because $[14]_{16}=[30]_{16}$ the equation $[6]_{16}X=[30]_{16}$ has as a solution $X=[5]_{16}$.

Proposition. *Suppose $X=x_0$ is a solution for $aX=b$. Let N be the set of all solutions to the homogeneous equation $aX=0$. Then every solution to $aX=b$ has the form $X=x_0+t$ for $t\in N$.*
Proof. If $a\,x_0=b$ and $at=0$, then $a(x_0+t)=b$. Conversely, to prove that all the solutions have such a form, let x_1 be another solution. Then $a(x_1-x_0)=b-b=0$, so $t=x_1-x_0$ is in N and $x_1=x_0+t$, as claimed.

Proposition. *If $d=(a,m)$, then the general solution in $\mathbb{Z}/m\mathbb{Z}$ of $[a]X=0$ is $X=[\frac{m}{d}k]$ for $k=0,\dots,d-1$.*
Proof. $ax\equiv 0\,(mod\,m)$ *iff* $ax=my$. Since $d=(a,m)$ then $\frac{a}{d}x=\frac{m}{d}y$. Now we have $(\frac{a}{d},\frac{m}{d})=1$, so should be $\frac{m}{d}|x$, and thus $x=\frac{m}{d}k$ for some integer k. So we've found that $X=[\frac{m}{d}k]$ for $k=0,\dots,d-1$. Note that if $k=d$ then $x=\frac{m}{d}\cdot d=m$, and $[m]=[0]$ (i.e. the solutions cyclically restart from the first class every d elements).

Unique inverse. We've already proven that if the inverse exists then is unique via a simple argument.
The uniqueness of inverse can be also proven using the previous proposition.
Proof. If $[a]$ is a unit in $\mathbb{Z}/m\mathbb{Z}$ then there exists an X such that $[a]X=[1]$ and this implies that $d=(a,m)=1$. Since $[a]X=[0]$ for $X=[\frac{m}{d}k]$ with $k=0,\dots,d-1$, in this case the only solution is $X=[0]$. Thus the equation $[a]X=[1]$ has a unique solution, i.e. the unique unit inverse.

Algebraic structures

A **group** is a set *G* together with a binary operation $*$ (called the **group law** of *G*) that combines any two elements *a* and *b* to form another element, denoted $a*b$.
Group axioms:

- **Closure**: for all *a, b* in *G*, $a*b$ is also in *G*
- **Associativity**: for all *a, b, c* in *G*, $(a*b)*c=a*(b*c)$
- **Identity** element: there exists an element *e* in *G*, such that $a*e=e*a=a$
- **Inverse** element: for each *a* in *G*, there exist an element a^{-1} such that $a*a^{-1}=a^{-1}*a=e$
- **Commutativity**: for all *a, b* in *G*, $(a*b)=(b*a)$

Depending on which axioms are satisfied, different *group-like* structures are defined:

- **Groupoid** (or magma): only closure is satisfied.
- **Semigroup**: an associative groupid.
- **Monoid**: a semigroup with identity.
- **Group**: a monoid with inverse.
- **Abelian group**: a commutative group.

Example. With the operation +, the set $\mathbb{Z}$ and $\mathbb{Q}$ are *Abelian* groups.
With the operation $\cdot$, the set $\mathbb{Q}$ is an *Abelian* group while the set $\mathbb{Z}$ not because only 1 and -1 elements have the multiplicative inverse..

Let *F* be a set along with with two operators: the product $\cdot$ and the addition +. If the set *F* is a group with respect to the two operators, with the only exception that 0 doesn't have a multiplicative inverse, then *F* is called a **field**. The addition and product identities are defined as 0 and 1, respectively.
A field should have the non-triviality property, i.e. *F* should have at least two elements.
For example, the set $\mathbb{Q}$ of rational numbers is a field.
The set $\mathbb{Z}$ of integers satisfies all properties required by a field except that not every element has a multiplicative inverse. If in a set *R* the multiplicative inverse may not be preset for some elements then the set *R* is called a **commutative ring.**
Note that a field posses the properties of a commutative ring, thus is also a commutative ring.

For example, the sets $\mathbb{Z}$ and $\mathbb{Q}$ are both commutative rings.

If *R* is a ring and *S* is a subset of *R* that is closed under addition, multiplication, taking negatives, and has 0 and 1, then *S* is also a ring. We call *S* a **subring** of *R*. Obviously, because it is a subset, the properties that hold in *R* hold in *S*.

Example. $\mathbb{Z}$ can be thought as a subset of $\mathbb{Q}$ by identifying the integer *a* with the rational number *a/1*. Then $\mathbb{Z}$ is a subring of $\mathbb{Q}$.

But $\mathbb{Z}/m\mathbb{Z}$ is not a subring of $\mathbb{Z}$ since $\mathbb{Z}/m\mathbb{Z}$ is not a subset of $\mathbb{Z}$. Rather, it is a set of subsets of $\mathbb{Z}$, the congruence classes of $\mathbb{Z}$ modulo *m*.

Theorem. *$\mathbb{Z}/\mathbb{Z}_m$ is a commutative ring with identity for every* $m \geq 2$.

Proof. We've defined $[a]+[b]=[a+b]$, $-[a]=[-a]$, $[a]\cdot[b]=[a\cdot b]$. Set $1=[1]$ and $0=[0]$. With these definitions is easy to show that since $\mathbb{Z}$ is a commutative ring with identity, then so is $\mathbb{Z}/\mathbb{Z}_m$.

For example. The commutative law for addition $[a]+[b]=[a+b]=[b+a]=[b]+[a]$; the identity for multiplication $[a]\cdot[1]=[a\cdot 1]=[a]$. The other properties are equally easy to verify.

Definition. *An element a of a commutative ring R is called a unit of R if there exists some b in R so that* $a\cdot b=b\cdot a=1$.

Example. In $\mathbb{Z}$ only 1 and -1 are units. In $\mathbb{Q}$ every nonzero number is a unit.

Units are **closed** under multiplication. That is if *a* and *b* are units of *R*, and a^{-1} and b^{-1} their inverses, then *ab* has an inverse, namely $b^{-1}a^{-1}$. Thus the units of a ring form a group U_R under multiplication. Note that U_R is not a field since $0 \notin U_R$.

If F is a group then the group of units U_F should contains all the *F's* elements except the 0.

Proposition. *A group has only one identity element.*

Proof. If e_0 and e_1 are both identity elements. Then $e_0 * e_1$ should be equal to both e_0 and e_1. Follows that $e_0 = e_1$.

Proposition. *In a group, an element has only one inverse.*

Proof. Given an element *a* in the group. If *b* and *c* are both inverses for *a*, then $a*b=e$ and $a*c=e$. Then $a*b=a*c$ and multiplying both sides by *b* we have $b*(a*b)=b*(a*c)=(b*a)*b=(b*a)*c$ for commutativity of the inverse $b*a=e$ then $b=c$.

This last proposition implies that in a ring, an element *a* has only one negative and, eventually, only one multiplicative inverse.

Zero divisors

Definition. A *non-zero* element *a* of a ring *R* for which there is some *non-zero b* such that *ab=0* is called a **zero divisor**.

NZD. A ring *R* for which for all *a, b in R if ab=0 then a=0 or b=0* is said to have no zero divisors.
Example. $\mathbb{Z}$ has no zero divisor.
Example. In $\mathbb{Z}/6\mathbb{Z}$, $[3][4]=[12]=[0]$, so both $[3]$ and $[4]$ are zero divisors.
Given $[a]_m \neq [0]_m$, any non-zero solution of $[a]_m X = [0]_m$ is a **complementary** zero divisor of $[a]_m$.
Example. in $\mathbb{Z}/12\mathbb{Z}$, $[6]$ has complementary zero divisors $[2],[4],[6],[8],[10]$.

Proposition (**Cancellation**). Non-zero divisors can be canceled. That is, l*et R be a commutative ring and suppose* $a \neq 0$ *in R is a non-zero divisor. Then if b, c are in R and ab=ac, then b=c.*
Proof. From *ab=ac* we obtain *ab-ac=0,* hence *a(b-c)=0.* Since *a* is not a zero divisor and *a(b-c)=0,* we must have *b-c=0,* and so *b=c.*

Corollary. *If a is not a zero divisor of a commutative ring R, then for all b in R, the equation ax=b has at most one solution.*
Proof. If $ax_1 = b$ and $ax_2 = b$, then $ax_1 = ax_2$. By cancellation $x_1 = x_2$.

A similar result holds for polynomial equations of higher degree.

(*) Proposition. *Let R be a commutative ring. If R has no zero divisors, then for every r, s in R, the equation* $x^2 - rx + s = 0$ *has at most two solutions in R. On the other hand, if R has non-zero elements a and b such that ab=0 and at least three of 0, a, b and a+b are distinct, then the equation* $x^2 - (a+b)x = 0$ *has at least three roots in R.*
Proof. Suppose *a* and *b* are complementary zero divisors in *R*, so that $a, b \neq 0$ and *ab=0*. Then it's easy to check that $x^2 - (a+b)x = 0$ has four solutions: *a, b, a+b* and *0*. So if at least three of these are distinct, then the equation has at least three distinct roots.
Conversely, suppose *R* has no zero divisors, and suppose $x^2 - rx + s = 0$ has two solutions *a, b:*

$a^2 - ra + s = 0$ and $b^2 - rb + s = 0$

Now suppose that there is a third solution *c*, so that $c^2 - rc + s = 0$.

Subtracting this last equation from each of the previous solutions we get

$r(a-c) = a^2 - c^2 = (a-c)(a+c)$ and $r(b-c) = b^2 - c^2 = (b-c)(b+c)$

Since *R* has no zero divisors if $c \neq a$ and $c \neq b$ we can cancel $a-c$ from the first equation and $b-c$ from the second, to get $r = a+c$ and $r = b+c$ which implies that $a=b$. Thus if $a \neq b$ then *c* must be equal to *a* or *b*, so there cannot be more than two solution to $x^2 - rx + s = 0$.

Proposition. *In a commutative ring R, if a is unit then a is not a zero divisor.*

Proof. Suppose *a* is a unit in *R*. We'll prove that if *ab=0*, then *b* must be zero. Suppose *ab=0*. Since *a* is a unit, there exits the inverse a^{-1}. Multiply both sides on the left by a^{-1} to get $a^{-1}(ab) = a^{-1}0 = 0$. Reassociating the left side, we have $(a^{-1}a)b = 0$, hence *b=0*.

Corollary. *A field has no zero divisors.*

Proof. In a field every element is a unit (has a multiplicative inverse), thus there are no zero divisors. The converse is not true. If a set has no zero divisor does not imply that is a field (e.g. $\mathbb{Z}$).

Theorem. *In* $\mathbb{Z}/m\mathbb{Z}$

i. if $(a,m) = 1$ *then* $[a]$ *is a unit;*

ii. if $1 < (a,m) < m$ *then* $[a]$ *is a zero divisor;*

iii. *if* $(a,m) = m$ *then* $[a] = 0$ ($m|a$).

Proof.

(*i*) Proved via the *Bezout's* identity $(a,m) = 1 \rightarrow 1 = as + mt \rightarrow [1] = [a][s]$.

(*ii*) Suppose $(a,m) = d$ and $1 < d < m$. Then *a* is not a multiple of *m*, so $[a] \neq [0]$. But since $d|m$, then there is a number *e* with $1 < e < m$ so $de = m$ and $[e] \neq 0$. Since $a = dk \rightarrow ae = dek = mk$ then *ae* is a multiple of *m*, so $[a][e] = [ae] = [0]$. Thus $[a]$ is a zero divisor.

(*iii*) If $m|a$ then $a \equiv 0 (mod\ m)$ and $[a] = 0$.

Corollary. $\mathbb{Z}/m\mathbb{Z}$ *is a field iff m is prime*.

Proof. If $[a]$ is any non-zero element of $\mathbb{Z}/m\mathbb{Z}$, then *m* doesn't divide *a (*contrapositive of *iii)*. If *m* is prime, follows that $(a,m) = 1$, hence $[a]$ is a unit. Thus every nonzero element of $\mathbb{Z}/m\mathbb{Z}$ is a unit, so $\mathbb{Z}/m\mathbb{Z}$ is a field. If *m* is not prime, then *m=ab* with $1 < a, b < m$; then $[a][b] = [m] = [0]$, while $[a]$ and $[b]$ are not zero. Thus $\mathbb{Z}/m\mathbb{Z}$ has zero divisors, and so cannot be a field.

Theorem. *If R is a finite commutative ring with identity, and a is any non-zero element of R, then a is either a unit or a zero divisor*.

Proof. Suppose *R* has *n* elements. Letting $a^s = a \cdots a$ (*s* factors) for any natural number *s*, and $a^0 = 1$, consider the set of elements $a^0, \ldots, a^n$. This is a set of *n+1* elements in *R*, a set of *n* elements. So, at least two of them should be equal. Suppose $a^r = a^{r+d}$ for some $r \geq 0$ and $d > 0$. Then $a^{r+d} - a^r = 0$, so $a^r(a^d - 1) = 0$. Choose *r* minimal so that $a^r(a^d - 1) = 0$. If $r = 0$, then $a^d - 1 = 0$, so $a(a^{d-1}) = 1$ and *a* is a unit of *R*. If $r > 0$, then (by minimality of *r*) $a^{r-1}(a^d - 1) \neq 0$, while $a(a^{r-1}(a^d - 1)) = 0$. Thus *a* is a zero divisor of *R*.

Order. The above theorem proof shows that if *a* is a unit then there is some *d>0* such that $a^d = 1$. The minimal such *d>0* is called the **order** of *a*.

Corollary. *A finite commutative ring with no zero divisors is a field.*

Note: the fact that $\mathbb{Z}$ has no zero divisors and only two units (± 1) is compatible with the theorem since it requires that *R* is finite. Follows that $\mathbb{Z}$ contains elements that are no-zero divisors nor units.

Corollary. *If a is a zero divisor it cannot have an inverse.*

Proposition. *If R is a ring with no zero divisors and S is a subring of R, then S has no zero divisors.*

Proof. If *S* is a subring of *R* then every *a, b* in *S* are in *R* as well. If in *R* do not exist $a, b \neq 0$ such that $ab = 0$ then they doesn't exist in *S* as well.

To find all the zero divisors in $\mathbb{Z}/m\mathbb{Z}$, first find the units U_m, then the zero divisors are $\mathbb{Z}/m\mathbb{Z} \setminus U_m$.

In $\mathbb{Z}/m\mathbb{Z}$ given a zero divisor $[a]_m$, the complementary zero divisors are found by finding the non-zero solutions to the general homogeneous equation $[a]_m X = 0$. We know the solution is $X = [\frac{m}{(a,m)}k]$ with $k = 1, \ldots, (a,m)$.

Equations

Proposition. *In a ring R, for any b, if the non-homogeneous equation* $ax=b$ *has some solution* $x=x_0$, *then the general solution to* $ax=b$ *is of the form* $x=x_0+t$ *where* t *is a solution of the homogeneous equation* $ax=0$.

Proof. If $ax_0=b$ and $at=0$ then $a(x_0+t)=b$. To show that every solution has that form consider another arbitrary solution x_1 such that $ax_1=b$. Then $a(x_1-x_0)=b-b=0$, thus $t=x_1-x_0$ is a solution to the homogeneous equation and $x_1=x_0+t$.

Because a field has no zero divisors, the equation $ax=0$ has only one solution $x=0$ and consequently the equation $ax=b$ has a unique solution.

Rings Homomorphism

Let R and S be two rings and f be a function from R to S. Then $f:R\to S$ is a **ring homomorphism** if f satisfies, for all a and b in R, the following properties:

i. $f(a+b)=f(a)+f(b)$
ii. $f(a\cdot b)=f(a)\cdot f(b)$
iii. $f(1)=1$
iv. $f(0)=0$
Follows from i, $f(b)=f(0+b)=f(0)+f(b)$, thus $f(0)$ should be 0
v. $f(-a)=-f(a)$
$0=f(0)=f(a+(-a))=f(a)+f(-a)$, the additive inverse is unique, thus $f(-a)=-f(a)$
vi. $f(a^{-1})=f(a)^{-1}$ (if the inverse of a exists)
$1=f(1)=f(a\cdot a^{-1})=f(a)\cdot f(a^{-1})$, the multiplicative inverse is unique, thus $f(a^{-1})=f(a)^{-1}$

A ring homomorphism f is one-to-one if f is one-to-one as a function.
Note that in iii and iv the left-hand side 1 and 0 are elements of R, thus they can be called 1_R and 0_R, the right-hand side 1 and 0 are elements of S, thus they can be called 1_S and 0_S.

Proposition. *A ring homomorphism f is one-to-one iff 0 is the only element a of R with* $f(a)=0$.
Proof. If $a\neq 0$ and $f(a)=0$, then since $f(0)=0$ f is not one-to-one. On the other hand, if f is not one-to-one, then there are two different elements a and b of R so that $f(a)=f(b)$.
But then $0=f(a)-f(b)=f(a-b)$ and a-b is not the zero element of R.

Definition. Let $f:R\to S$ be a homomorphism. The **kernel** of *f*, written $ker(f)$, is the set of elements $r\in R$ so that $f(r)=0$. Concisely, $ker(f)=\{r\in R: f(r)=0\}$.
The size of $ker(f)$ describes how far *f* is from being one-to-one. If $ker(f)=\{0\}$ then is one-to-one.

Proposition. *Let $f:R\to S$ be a ring homomorphism and let s be in the image of f.*
Then $\{r\in R: f(r)=s\}$ is in a one-to-one correspondence with $ker(f)$.
Proof. It is easy to see that if $f(r_0)=s$, then $\{r\in R: f(r)=s\}=\{r_0+k: k\in ker(f)\}$. That is, $f(r_0)=s$ and $f(k)=0$ then $f(r_0+k)=f(r_0)+f(k)=s+0=s$

Corollary. If $ker(f)$ has *m* elements then *f* is an ***m-to-one*** function.

Proposition. *Let $f:R\to S$ be a homomorphism where R is a <u>field</u> and $1\neq 0$ in S. Then f is one-to-one.*
Proof. Suppose $a\neq 0$ in *R*, we show that $f(a)\neq 0$. Since *R* is a field, *a* has an inverse a^{-1}. Then $1=f(1)=f(a\cdot a^{-1})=f(a)\cdot f(a^{-1})$. If $f(a)=0$ then 1=0, and this is impossible since by hypothesis $1\neq 0$ in S. Thus the kernel contains only 0 and *f* is one-to-one.

Homomorphisms with domain $\mathbb{Z}$

Proposition. *The function $\mathbb{Z}\to R$ defined by $f(n)=n\cdot 1_R$, $f(1)=1_R$ is a homomorphism and is the only ring homomorphism from $\mathbb{Z}$ to R.*
Proof. To prove that it is a homomorphism we need to check the properties i, ii and iii.

i. for any *m, n* in $\mathbb{Z}$ $f(m+n)=f(m)+f(n)$
   $(m+n)\cdot 1_R=m\cdot 1_R+n\cdot 1_R$ this immediately follows from the distributive law in *R*.

ii. for any *m, n* in $\mathbb{Z}$ $f(m\cdot n)=f(m)\cdot f(n)$
   $(m\cdot n)\cdot 1_R=m\cdot 1_R\cdot n\cdot 1_R$ this follows the distributive law in *R*
   $n\cdot 1_R=1_R+\ldots+1_R$ (*n summands*) and so
   $$\begin{aligned}(m\cdot 1_R)(n\cdot 1_R)&=(m\cdot 1_R)(1_R+\ldots+1_R)=\\ &=(m\cdot 1_R)+\ldots+(m\cdot 1_R)=\quad (n\ \ summands)\\ &=1_R+\ldots+1_R=\qquad\quad (m\,n\ \ summands)\\ &=(m\cdot n)\cdot 1_R\end{aligned}$$

iii. $f(1)=1\cdot 1_R=1_R$. This is trivially true by definition.

To prove that is the only ring homomorphism, we must show that if *f* is a homomorphism from $\mathbb{Z}$ to *R*, then $f(n)=n\cdot 1_R$. The proof is by induction.

Given that $f(1)=1_R$ and assuming that for $k\geq 1$, $f(k)=k\cdot 1_R$. Then $f(k+1)=f(k)+f(1)=f(k)+1_R$. Then for any n>0, $f(n)=n\cdot 1_R=1_R+\ldots.+1_R$. Since the definition $f(n)=n\cdot 1_R$ is forced by the condition that *f* is a homomorphism, then this is the only ring homomorphism.

For example.

1. If $R=\mathbb{Z}$ then the homomorphism $f:\mathbb{Z}\to\mathbb{Z}$ is defined by $f(n)=n\cdot 1=n$
2. If $R=\mathbb{Q}$ then the homomorphism $f:\mathbb{Z}\to\mathbb{Q}$ is defined by $f(n)=n\cdot 1/1=n/1$
3. If $R=\mathbb{Z}/m\mathbb{Z}$ then the homomorphism $f_m:\mathbb{Z}\to\mathbb{Z}/m\mathbb{Z}$ is defined by $f(n)=n\cdot[1]_m=[n]_m$

Note that f_m is onto but not one-to-one. In fact, two integers that are congruent modulo *m* are mapped by f_m to the same congruence class. The kernel of f_m is the infinite set of integers multiples of *m*. That is $ker(f_m)=\{x\in\mathbb{Z}:\ f_m(x)\in[0]_m\}$.

Ring characteristic

Definition. Let $f:\mathbb{Z}\to R$ be a homomorphism. If *f* is one-to-one then *R* is said to have **characteristic zero**.

If f is not one-to-one then there is some non-zero integer c in the $ker(f)$. If $f(c)=0$, then $f(-c)=-f(c)=-0=0$, so there is a natural number in $ker(f)$.

Proposition. If $f:\mathbb{Z}\to R$ is a homomorphism and *m>0* is the smallest natural number in $ker(f)$, then $ker(f)$ is the set of integers that are multiples of *m*.

Proof. If *b* in $ker(f)$, then divide *b* by *m*: $b=mq+r$ where $0\leq r<m$. Applying *f* to the equation we have: $0=f(b)=f(m)f(q)+f(r)=0\cdot f(q)+f(r)=f(r)$. Thus *r* should be zero and *b* is a multiple of *m*.

Let *m* be the smallest natural number in $ker(f)$ and $m\mathbb{Z}$ be the set of all multiples of *m*.

Proposition. *Let R be a commutative ring with no zero divisors, and* $f:\mathbb{Z}\to R$. *If* $ker(f)=m\mathbb{Z}$ *and* $m\neq 0$, *them m is prime.*

Proof. If *m* is not prime, then *m=ab*, with $0<a<m$ and $0<b<m$. Then $f(a)\neq 0$, $f(b)\neq 0$, but $0=f(m)=f(ab)=f(a)f(b)$, so *R* has zero divisors.

Definition. If *R* has no zero divisors, and $f:\mathbb{Z}\to R$ by $f(n)=n\cdot 1_R$ is not one-to-one, then $ker(f)=p\mathbb{Z}$ where *p* is a prime number. In that case we say that *R* has **characteristic *p*.**

Corollary. *Any field, a ring with no-zero divisors (all elements are units), has either characteristic zero or p for some prime p.*

Corollary. *If F is a field with a finite number of elements, then F has characteristic p for some prime number p.*

Proof. Since $\mathbb{Z}$ has an infinite number of elements, then $f:\mathbb{Z}\to R$ cannot be one-to-one and thus cannot have characteristic zero. The thesis follows, by exclusion, from the previous corollary.

Isomorphism

Definition. A ring homomorphism $f:R\to S$ is an *isomorphism* if f is one-to-one and onto. Two rings R and S are isomorphic if there is an isomorphism between them.

Two isomorphic groups from an abstract point of view are "equal". That is they can be manipulated in the same way.

Proposition. *Let R be a commutative ring and let $f:\mathbb{Z}\to R$ be the homomorphism defined by $f(n)=n\cdot 1_R$ for all n in $\mathbb{Z}$. If f is one-to-one, so that R has characteristic zero, then f defines an isomorphism from $\mathbb{Z}$ onto $\{n\cdot 1_R:\ n\in\mathbb{Z}\}\subseteq R$.*

Proof. If R has characteristic zero. A function maps onto its image. Thus if f is a one-to-one homomorphism, then f is an isomorphism from its domain to its image.

For example: $f:\mathbb{Z}\to\mathbb{Q}$ is an isomorphism from $\mathbb{Z}$ onto $\{n\cdot 1/1:\ n\in\mathbb{Z}\}\subseteq\mathbb{Q}$ but not onto $\mathbb{Q}$.

(rivedi) Homomorphism Theorem. Let R be a commutative ring and let $f:\mathbb{Z}\to R$ be the homomorphism defined by $f(n)=n\cdot 1_R$ for all n in $\mathbb{Z}$. If f is not one-to-one and $m\mathbb{Z}\subseteq ker(f)$ for some $m\neq 0$ in $\mathbb{Z}$, then f induces a homomorphism $\bar{f}$ from $\mathbb{Z}/m\mathbb{Z}$ onto $\{n\cdot 1_R:\ n\in\mathbb{Z}\}\subseteq R$, defined by $\bar{f}([a]_m)=f(a)=a\cdot 1_R$.
If $ker(f)=m\mathbb{Z}$ then $\bar{f}$ is an isomorphism from $\mathbb{Z}/m\mathbb{Z}$ onto $\{n\cdot 1_R:\ n\in\mathbb{Z}\}\subseteq R$
Proof. **… ???**

(rivedi) Corollary. *Let R be a commutative ring with no zero divisors. If R has characteristic zero, then R contains a subring isomorphic to $\mathbb{Z}$. If R has characteristic p, a prime, then R contains a subring isomorphic to $\mathbb{Z}/p\mathbb{Z}$.*

(rivedi) Corollary. *If d, m are integers and* $d|m$ *, then the homomorphism* $f:\mathbb{Z}\to\mathbb{Z}/d\mathbb{Z}$ *defined by* $f(n)=n\cdot 1$ *induces a homomorphism* $\bar{f}:\mathbb{Z}/m\mathbb{Z}\to\mathbb{Z}/d\mathbb{Z}$ *, and a map from* U_m *, the group of units of* $\mathbb{Z}/m\mathbb{Z}$ *, onto* U_d

Fermat's and Euler's Theorems

Order of Elements

There are exactly *m* congruence classes modulo *m*. If we look at the powers of *a*: $1,a,a^2,a^3,\ldots,a^m$, then since there are $m+1$ powers and *m* congruence classes, at least two of the powers must be in the same congruence class.

Suppose $a^r\equiv a^s(mod\,m)$ for some $r\geq 0$ and $s>r$. Then $a^{t+k}\equiv a^{s+k}(mod\,m)$ for every $k\geq 0$. So from a^s on the powers of a modulo *m* repeat earlier powers of *a*.

Proposition. *If a and m are coprime, then* $a^t\equiv 1(mod\,m)$ *for some t,* $0<t<m$.

Proof. Since $(a,m)=1$ then *m* does not divide a^s for any *s*, and so the *m* numbers $1,a,a^2,\ldots,a^{m-1}$ all belong to the $m-1$ congruence classes other than the congruence class of 0. So two of the numbers must be in the same congruence class: there are numbers *s* and *t* with $s\geq 0$ and $0<t<m$ so that $a^s\equiv a^{s+t}(mod\,m)$. Since *a* and *m* are coprime the cancellation property holds and we can cancel the common factor a^s from both sides to get $1\equiv a^t(mod\,m)$.

In other words, if $[a]_m$ is a unit then $[a^t]_m=[1]_m$ for some *t* with $0<t<m$.

Order. Let $m>1$ and *a* be any integer coprime to *m*. The order of *a* modulo *m* is the smallest positive integer *e* so that $a^e\equiv 1(mod\,m)$.

Existence. We know that if $(a,m)=1$ then there is a positive exponent *t*, $0<t<m$, such that $a^t\equiv 1(mod\,m)$. Hence by *WOP* there is the least one.

Proposition. *If e is the order of a modulo m, and* $a^f \equiv 1 (\mathit{mod}\, m)$ *, then e divides f.*

Proof. Divide e into f to get $f=eq+r$, with $0 \le r < e$. Then $a^f \equiv (a^e)^q \cdot a^r \equiv 1^q \cdot a^r \equiv a^r (\mathit{mod}\, m)$, so $a^r \equiv 1 (\mathit{mod}\, m)$. But $r<e$ and e is the least positive number with $a^e \equiv 1 (\mathit{mod}\, m)$. So $r=0$ and e divides f.

Proposition. *If a has order e modulo m and* $d>0$ *, then the order of* a^d *modulo m is* $e/(d,e)$.

Proof. Recall that $de=[d,e](d,e)$ or that $e/(d,e)=[d,e]/d$. Since e divides $[d,e]$ and $a^e \equiv 1 (\mathit{mod}\, m)$, we have $a^{[d,e]} \equiv (a^e)^k \equiv 1 (\mathit{mod}\, m)$. Follows that $(a^d)^{\frac{[d,e]}{d}} \equiv (a^d)^{\frac{e}{(d,e)}} \equiv 1 (\mathit{mod}\, m)$. To show that is the order of a^d, suppose that $(a^d)^s \equiv 1 (\mathit{mod}\, m)$ for some $s>0$. Then $a^{ds} \equiv 1 (\mathit{mod}\, m)$. Since e is the order of a, then e divides ds. So ds is a common multiple of d and e, so $ds \ge [d,e]$, hence $s \ge [d,e]/d = e/(d,e)$.

Fermat's Theorem

Fermat's Theorem. *If p is a prime and a is an integer not divisible by p, then* $[a]_p^{p-1} = [1]_p$.

Proof. Write the multiplication table for $\mathbb{Z}/p\mathbb{Z}$ (we omit the brackets $[\ ]_p$ in the table)

·	*1*	*2*	*3*	...	*p-1*
1	*1*	*2*	*3*	...	*(p-1)*
2	*2*	*2 · 2*	*2 · 3*	...	*2 · (p-1)*
3	*3*	*3 · 2*	*3 · 3*	...	*3 · (p-1)*
⋮	⋮	⋮	⋮		⋮
a	*a*	*a · 2*	*a · 3*	...	*a · (p-1)*
⋮	⋮	⋮	⋮		
p-1	*p-1*	*(p-1) · 2*	*(p-1) · 2*	...	*(p-1) · (p-1)*

Let U be the set of all the non-zero elements in $\mathbb{Z}/p\mathbb{Z}$. For any $[a] \ne [0]$ let $a \cdot U$ denote the set where each element of U is multiplied by $[a]$. Because $(a,p)=1$, then $[a]$ is a unit in $\mathbb{Z}/p\mathbb{Z}$. Given $[u]$ an arbitrary element of U, then $[u]=[1][u]=[a][a^{-1}][u]=[a][a^{-1}u]$. Since a^{-1} is a unit as well, for closure of the set of units U: $[a^{-1}u] \in U$. Follows that $[u] \in a \cdot U$ and thus that U is a subset of $a \cdot U$. Thus U and $a \cdot U$ both have *p-1* elements. Follows that $aU = U$.

The product of the elements of $a \cdot U$ is $[a \cdot 1] \cdot [a \cdot 2] \cdot [a \cdot 3] \cdots [a \cdot (p-1)] = [a^{p-1}][1 \cdot 2 \cdot 3 \cdots (p-1)]$.

While the product of the elements of U is $[1 \cdot 2 \cdot 3 \cdots (p-1)]$.

Because $aU = U$ then $[a^{p-1}][1 \cdot 2 \cdot 3 \cdots (p-1)] = [1 \cdot 2 \cdot 3 \cdots (p-1)] \rightarrow [a^{p-1}] = [1]$.

Corollary. *If p is prime and a is not divisible by p, then the order of a divides p-1.*
Proof. Immediately follows from the Fermat's Theorem and the already proven order property: if e is the order of a, and $[a^f]=[1]$, then $e|f$.

Corollary. *If p is prime, then for any number a,* $[a^p]=[a]$.
Proof. If $(a,p)=1$ then, since $[a^{p-1}]=[1]$, multiplying both sides by a we get $[a^p]=[a]$. If $(a,p)\neq 1$ then $p|a$ thus $[a]=[0]$ and $[a^p]=[a]$.

Euler's Theorem. *For every unit* $[a]$ *of* $\mathbb{Z}/m\mathbb{Z}$*:* $[a]^{\phi(m)}=[1]$
Proof. Let U be the set of $\phi(m)$ units modulo m and $a\cdot U$ the set where each unit of U has been multiplied by a, with $[a]$ a unit of U. Given $[u]$ an arbitrary element of U, then $[u]=[1][u]=[a][a^{-1}][u]=[a][a^{-1}u]$, so $[u]\in a\cdot U$. The argument proceeds similarly to the Fermat's theorem proof by observing that $U=a\cdot U$ both have $\phi(m)$ elements.

Notice that Fermat's theorem is a special case of Euler's theorem. If m is prime then $\phi(m)=m-1$.

Corollary. *If (a,m)=1, then the order of a divides* $\phi(m)$.
Corollary. *If (a,m)=1, then for any number a,* $[a^{\phi(m)+1}]=[a]$.

Corollary. If $[a]$ is a unit modulo m. The inverse of $[a]$ is $[a^{\phi(m)-1}]$.
Proof. Immediately follows the Euler's Theorem.

Montgomery reduction

Given the modulus m, we can choose a radix $r>m$ such that m is coprime to r, and such that finding the least non-negative residue of any number modulo r is easy.
Let b be a number $<rm$. We want to find b modulo m without never dividing by m directly.

Initialization
Since m and r are coprime, we can find r' and m' so that $rr'=1+mm'$, where $0<r'<m$ and $0<m'<r$. We also find the least non-negative residue w of r^2 modulo m.

First part: find $br' \bmod m$.

Let >> $s = bm' \bmod r$ << then multiplying by m yields $sm \equiv bmm' \pmod{rm}$.

Since $s<r$ then $sm<rm$ and sm is the largest non-negative residue of bmm' modulo rm. Then

$$b + sm \equiv b + bmm' = b(1 + mm') = brr' \pmod{rm}$$ (that is why we require that $(r, m) = 1$)

So $b+sm$ is a multiple of r. Divide the congruence by r, to get >> $z = (b + sm)/r$ <<.

Then $z \equiv br' \pmod{m}$ and we also have that $z<2m$.

To see that $z<2m$ recall that $b<rm$ by assumption, and $sm<rm$. So $rz = b + sm < 2rm$, hence $z<2m$.

The last non-negative residue c of $br' \bmod m$ is then either z, if $z < m$, or $z-m$, if $m \le z < 2m$.

Second part: find $b \bmod m$.

Multiply c by w, then $cw \equiv br'r^2 \equiv br \pmod{m}$.

If we then repeat the first part for cw instead of b, we will end up with a number $d<m$ such that

$$d \equiv cwr' \equiv br'r^2r' \equiv b \pmod{m}$$

Note that we're arrived to the result without never directly dividing by m.

Algorithm Outline

- $s = bm' \bmod r$
- $z = (b + sm)/r$, $z < 2m$
- $c=z$, if $z < m$, or $c=z-m$, if $m \le z < 2m$.
- $s' = cwm' \bmod r$
- $z' = (cw + s'm)/r$, $z' < 2m$
- $d = z'$, if $z' < m$, or $c = z' - m$, if $m \le z' < 2m$.
- $d = b \bmod m$

RSA cryptosystem

Bob chooses two different large primes p and q that he keeps secret, and sets $m=pq$. He chooses an encrypting exponent e coprime to $\phi(m) = (p-1)(q-1)$. Then Bob finds a number d such that

$$ed \equiv 1 \pmod{\phi(m)}$$

Then d is the inverse of e modulo $\phi(m)$. Bob can find d by solving the equation

$$ed + \phi(m)k = 1$$

Since e and $\phi(m)$ are coprime, the equation can be solved by the extended Euclidean Algorithm.

$$ed = 1 + \phi(m)k$$

Bob keeps *d* secret but broadcasts *m* and *e* to Alice.

Alice has a message consisting of a sequence of words. Each word is a number *w* less than *m*. To encrypt a word Alice computes:

$$c = w^e \bmod m$$

That is, Alice finds the number $c<m$ that is congruent to w^e modulo *m*.

To decrypt the ciphertext, Bob computes

$$w = c^d \bmod m$$

For since $ed \equiv 1 \pmod{\phi(m)}$, we have

$$c^d = (w^e)^d = w^{1+\phi(m)k} \equiv w \cdot w^{\phi(m)k} \equiv w \pmod m$$

If the factorization of m is known then $\phi(m)$ can be found instantly and the decoding exponent *d* can be found by Euclid's algorithm in a few seconds. Thus the effectiveness of the RSA cryptosystem ultimately lies in the fact that factoring large numbers into products of primes is an inefficient computational process.

Pseudoprimes

The most naive approach to test if a number is prime is by trial division. If a number m is not divisible by any prime $\leq \sqrt{m}$ then is prime.

Fermat's theorem says that if *m* is a prime number and *a* an integer relatively prime to *m*, then *m* divides $a^{m-1}-1$. The contrapositive is

Proposition. *If $a^{m-1}-1$ is not divisible by m, then m is not prime.*

The $(a,m)=1$ condition has been removed. Indeed if $(a,m)\neq 1$ then *m* is not prime anyway.

The ***2-pseudoprime test***. If $2^{m-1}-1$ is not divisible by *m*, then *m* is not prime.

If a number is prime then *m* passes the *2-pseudoprime test*, but the converse is not true.

A number *m* is a ***2-pseudoprime*** if is composite and passes the *2-pseudoprime test:* $2^{m-1} \equiv 1 \pmod m$.

Has been empirically proved that a randomly chosen number that satisfies the *2-pseudoprime* test is likely to be prime.

Note that no even number can pass the test: if $m=2k$ and $(m=2k)|(2^{m-1}-1)$ then an odd number is divisible by an even number. That is impossible.

Proposition. *If a number of the form* a^n-1 *is prime, then a=2 and n is prime.*
Proof.
i. In general $a^n-1=(a-1)(a^{n-1}+a^{n-1}+...+1)$, thus $(a-1)|(a^n-1)$. Because a^n-1 is prime, the only option is that *a-1=1*, that is *a=2*.
ii. If *n* is not prime then *n=xy* and $(a^n-1)=(a^{xy}-1)=(a^x-1)((a^x)^{y-1}+(a^x)^{y-2}+\ldots+1)$. Thus a^x-1 divides a^n-1.

A *perfect number* is equal to the sum of its proper divisors. For example 6=1+2+3.

Proposition. If 2^n-1 is prime, then $m=2^{n-1}(2^n-1)$ is a perfect number.
Proof. TODO?

Proposition. *If n passes the 2-pseudoprime test, then* 2^n-1 *does also.*
Proof. By hypothesis $n|(2^{n-1}-1)$ then $2^{n-1}-1=nk$ for some integer k. To prove that 2^n-1 passes the *2-pseudoprime* test we must show that $(2^n-1)|(2^{(2^n-1)-1}-1)$.
$2^{(2^n-1)-1}-1=2^{2(2^{n-1}-1)}-1=2^{2nk}-1=(2^n)^{2k}-1=(2^n-1)((2^n)^{2k-1}+(2^n)^{2k-2}+...+1)$.
Thus if *n* is prime, 2^n-1 is either prime or a *2-pseudoprime*.

Marsenne numbers. An integer sequence defined as $M_n=2^n-1$.

Fermat numbers. An integer sequence defined as $F_n=2^{2^n}+1$.

Proposition. If a number of the form $F_n=2^a+1$ is prime then *a* must be of the form 2^n for some *n*.

Proposition. *Every Fermat number passes the 2-pseudoprime test.*
Proof. We have to prove that $2^{F_n-1}\equiv 1(mod\ F_n)$ or more explicitly that $2^{(2^{2^n}+1)-1}=2^{2^{2^n}}\equiv 1(mod\ F_n)$.
Because $(a-1)\equiv -1(mod\ a)$ then $F_n-1\equiv -1(mod\ F_n)$ or $2^{2^n}\equiv -1(mod\ F_n)$.
Raising both sides by $2^{(2^n-n)}$ we get $(2^{2^n})^{2^{(2^n-n)}}=2^{2^{(n+2^n-n)}}=2^{2^{2^n}}=2^{F_n-1}\ \equiv\ (-1)^{2^{(2^n-n)}}=1\ \ (mod\ F_n)$.

If a number *m* is not prime and $m|(a^{m-1}-1)$ then we say that *m* passes the ***a-pseudoprime*** test and *m* is an **a-pseudoprime**.

Carmichael numbers. A composite number *m* is a Carmichael number if *m* is *a-pseudoprime* for every number *a* coprime to *m*.
By the Fermat's theorem we know that if *m* fails the *a-pseudoprime* test for a single number $a<m$ then *m* is composite.
The existence of Carmichael numbers dashes the hope that Fermat's Theorem alone can be used as a primality test. If *m* is a Carmichael number then no amount of *a-pseudoprime* testing will reveal that *m* is composite (unless we are lucky enough to pick *a* not coprime to *m*).

Pollard p-1 factoring algorithm

Let *k* be a number ≥ 2. A number *m* is **k-smooth** if every prime divisor of m is $\leq k$.
The larger k is, the more k-smooth numbers there are.

Groups

The properties we've seen so far, as the Euler's theorem, holds for any group *G*.

Abstract Fermat Theorem. *Let G be an abelian group with n elements. Then for any a in G,* $a^n=e$, *the identity element of G.*
Proof. Let $u_1,\ldots,u_n$ be the elements of *G*, and let *a* be any element of *G*. Consider the set $aG=\{au_1,\ldots,au_n\}$. Then *aG* is exactly the same as the set *G*: all the elements of *aG* are distinct and every element of *G* is in *aG*. Now multiply the elements of *aG* together and all the elements of *G* together, equate the two products and cancel the common factors. We'll be left with $a^n=e$.

The proof is supported by the following two properties.

Generalized Associativity. *If G is a group, so that* $a(bc)=(ab)c$ *for all a, b, c in G, then for every n>3 all possible ways of associating the product of every n elements of G are equal.*

Proof. By induction, we assume the result true for $m<n$ and we prove it for *n*.

We show that any way of parenthesization of the product $a_1 a_2 \cdots a_n$ is equal to the left-associated expression $(...((a_1 a_2)a_3)\ldots a_n)$. For any form of parenthesized expression there is an outermost multiplication, thus we can split the expression in two: $AB=(a_1 \cdots a_m)(a_{m+1} \cdots a_n)$ both parenthesized in some arbitrary way. Applying the inductive hypothesis we can rewrite the sub-expressions as left-associated expressions $A=(...((a_1 a_2)a_3)\ldots a_m)$ and $B=(...((a_{m+1} a_{m+2})a_{m+3})\ldots a_n)$.

If *B* is composed by a single element we are already done; else we can write *AB* as $A(C\,a_n)$, where C is still a left associated expression, and (base case) rewrite the expression as $(AC)a_n$. At this point we can repeat the process for *AC*. Following the algorithm we end up with a left-associated expression equivalent to the original one.

Generalized Commutativity. *If G is an abelian group, so that* $ab=ba$ *for all a, b in G, then for every n>2, all possible ways of multiplying n elements* $a_1,\ldots,a_n$ *of G, regardless of order, give the same element of G.*

Proof. Call the product $w=a_1 v$ apply induction to *v*. If $w=c\,a_1 b$, we use commutativity to get $w=a_1 cb$ and apply induction to *cb*.

If *G* is the group U_m of the $\phi(m)$ units of $\mathbb{Z}/m\mathbb{Z}$ for *m* any number ≥ 2, we have Euler's theorem.

Subgroups

Definition. Let *G* be a group with operation * and identity *e*. A subgroup *H* of *G* is a nonempty subset of *G* with two properties:

i. if *a, b* are in *H*, then *a*b* is in *H*

ii. if *a* is in *H* so is a^{-1}

The two properties together imply that $e\in H : (a\in H \rightarrow a^{-1}\in H) \rightarrow a*a^{-1}=e\in H$.

Example. If $G=\mathbb{Z}$ and the operation is +, then $m\mathbb{Z}$, the set of multiples of *m*, is a subgroup of *G*.

$a=ms$ and $b=mt$ then $a+b=m(a+t)=mk\in m\mathbb{Z}$

$a=mk\in m\mathbb{Z}$ then $a^{-1}=m(-k)\in m\mathbb{Z}$

Trivial subgroups of *G* are *G* itself and the subgroup consisting only of the identity element of *G*.

Cyclic Subgroup. Let *G* be a group with operation * and identity *e*. Fix an element *a* of *G*. The cyclic subgroup generated by *a* is the set *H* of elements of *G* of the form a^n for all integers *n*. Here a^0 denotes the identity element *e*, a^n *n>0* denotes $a*\ldots*a$, and a^{-n} for *n>0* denotes $a^{-1}*\ldots*a^{-1}$.
The cyclic subgroup of *G* generated by *a* is denoted by $\langle a\rangle$.
A group *G* is cyclic if $G=\langle a\rangle$ for some *a* in *G*.

Example. If $G=\mathbb{Z}$ and the operation is +, then the cyclic subgroup $\langle m\rangle$ generated by the integer *m* is $m\mathbb{Z}$, the set of all integers *rm*, where *r* is any element of $\mathbb{Z}$.

$m^n=m+\ldots+m=nm$

Proposition. *Suppose G is a finite group with n elements. Every element a of G has an order d* $\leq n$ *(* $a^d=e$ *, the identity of G, see the Zero Divisors chapter). If a has order d, then the cyclic subgroup* $\langle a\rangle$ *of G has d elements.*

$\langle a\rangle=\{a,a^{2,}...,a^d\}$

Hence the order of a is equal to the number of elements in $\langle a\rangle$.

Proof. Let *d* be the order of *a*, and let $A=\{a^{1,}\ldots,a^d\}$ where $a^d=a^0=e$. For every $k>0$, $k=dq+r$ with $0\leq r<d$. Then $a^k=a^{dq}a^r=a^r$ and *A* contains every positive power of *a*. In particular *A* is closed under the operation *. Also, for each *r* with $1\leq r<d$, $a^r a^{d-r}=a^d=e$ (Note: a^d is its own inverse). So all the inverses are in *A* as well. Follows that *A* is a subgroup of *G*.
Is left to show that all the elements of $\langle a\rangle$ are all different. Suppose that $a^s=a^{s+k}$ where $1\leq s<s+k\leq d$. Then, canceling a^s we have that $e=a^k$. But since $1\leq k<d$ this last equation violates that *d* is the order of *a*. Hence the elements in $\langle a\rangle$ are all different and their number is equal to the order *d*.

Proposition. *If* $\langle a\rangle$ *is a cyclic subgroup of G of order m=rs, then* $\langle a^r\rangle=\{a^r,a^{2r},\ldots,a^{sr}\}$ *is a cyclic subgroup of* $\langle a\rangle$*, hence a cyclic subgroup of G, of order s.*
Proof. Trivially prove that has the two subgroup properties and that has *s* elements.

Most groups have subgroups other than the trivial subgroups.

Proposition. *If G is an abelian group then G has a non-trivial subgroup unless the order n of G is 1 or a prime p.*

Proof. For each $a \neq e$ in *G*, consider the subgroup $\langle a \rangle$ generated by *a*. If $\langle a \rangle \neq G$ then it is a non-trivial subgroup of *G*. If $\langle a \rangle = G$ and $n=rs$ with $r, s > 1$, then $\langle a^r \rangle$ has order *s*, so is a proper subgroup of *G*. Thus if *G* has only trivial subgroups, then the order of *G* should be 1 or a prime (or infinite?).

For the previous proposition we have that a sufficient condition for a cyclic subgroup $\langle a \rangle$ to have a non trivial subgroup is that its order *m* is a composite number, $m=sr$. In such a case a cyclic subgroup can be easily defined as $\langle a^r \rangle$. But are all its subgroups cyclic?

Proposition. *A subgroup of a cyclic group* $\langle a \rangle$ *is cyclic.*

Proof. Let *H* be a subgroup of $\langle a \rangle$. If $H = \{ e = a^d \}$ then it is cyclic subgroup generated by a^d.

Let $H \neq \{ e = a^d \}$. By definition of a cyclic group every element of $\langle a \rangle$ has the form a^n. Then, as *H* is a subgroup of $\langle a \rangle$, the same holds for *H*, $a^n \in H$ for some $n \in \mathbb{Z}$. Let *m* be the smallest positive integer such that $a^m \in H$. Consider an arbitrary element $b \in H$, for what we just said, $b = a^n$ for some $n \in \mathbb{Z}$. For the division theorem $n = mq + r$ with $0 \leq r < m$. Follows that $a^n = (a^m)^q a^r$ and hence $a^r = a^n (a^m)^{-q}$, since $a^m \in H$ so is its inverse $(a^m)^{-1}$ and all powers of its inverse (for closure).

Since both a^n and $(a^m)^{-q}$ are in *H,* again for closure, $a^r \in H$. However since *m* was selected to be the smallest positive integer such that $a^m \in H$ and $0 \leq r < m$, then should be *r=0*. Follows that $b = a^n = (a^m)^q$ is a power of a^m. By the definition $H = \langle a^m \rangle$ is cyclic.

Proposition. *When G is a <u>finite</u> group with operation *. Then a non empty subset H of G is a subgroup iff H is closed under * (there is no need to include the inverse condition).*

Proof. If *G* is a finite group with *n* elements then an arbitrary element *a* has an order $d<n$. Thus the inverse of *a* is trivially defined as a^{d-1}.

The inverse existence that is implicit derived from the fact that G is finite, thus every element has an order *d*.

Cosets and Lagrange's Theorems

Left Coset (Definition). *Let G be a group with operation *, and H a subgroup. For any b in G, the left coset of b, denoted b*H, is the set of elements b*h where h runs through all elements of H*

$$b * H = \{ b * h : \ h \in H \}$$

Because only *H* contains the identity element, only *H* is a subgroup while the other cosets are not.

Example. Let $G=\mathbb{Z}$, $H=m\mathbb{Z}$ for some $m>1$ and the operation * is +. If a is any integer, then $a+m\mathbb{Z}$, the left coset of a, is the set of integers of the form $a+mk$ for k any integer, that is the set of integers congruent to a modulo m. Then the coset $a+m\mathbb{Z}$ is equal to the coset $b+m\mathbb{Z}$ *iff* a is congruent to b modulo m. There are m cosets, namely: $0+m\mathbb{Z}$, $1+m\mathbb{Z}$, … , $(m-1)+m\mathbb{Z}$. This is because any integer is congruent modulo m to exactly one of the numbers $0,1,\ldots,(m-1)$.

Proposition. *Let H be a subgroup of a group G. Two left cosets are either disjoint or equal.*

Proof. Suppose $a*H$ and $b*H$ have some element c in common. Then $c=a*h_i=b*h_j$, for some $h_i, h_j\in H$. We show that $a*H$ is thus contained in $b*H$. We know that $a*h_i=b*h_j$ is in $b*H$. Let $a*h'$ be any element of $a*H$. Then, since H is a group, we can find some t in H so that $h_i*t=h'$. But then $a*h'=a*h_i*t=b*h_j*t$, an element of $b*H$. So $a*H\subseteq b*H$. In a similar way we can prove that $b*H\subseteq a*H$. Thus $a*H=b*H$.

Proposition. *If a*H is any coset of H, then the number of elements in a*H is equal to the number of elements in H.*

Proof. The idea is to define a bijective function T from H to $a*H$ by the rule, $T(h)=a*h$. To see that T is a bijection, observe that we can define an inverse function S from $a*H$ to H as

$$S(a*h)=a^{-1}*(a*h)=(a^{-1}*a)*h=e*h=h$$

So the composition $S\circ T$ is the identity function on H.

If G is an abelian group with n elements, when for any a in G, the order of a divides n. The number of elements of the subgroup generated by an element $a\in G$ is equal to the order of a. Thus the number of elements of $\langle a\rangle$ divides n.

Lagrange's Theorem. *Let G be a <u>finite</u> group and H a subgroup of G. Then the number of elements of H divides the number of elements of G.*

Proof. Let G have n elements and H have m elements. Write G as a union of left cosets

$$G=(a_1*H)\cup(a_2*H)\cup\ldots\cup(a_n*H)$$

Unless H contains only the identity element, there will be cosets elements in this union that are equal. So starting from the coset a_2*H, look at each coset $a_{k+1}*H$ to see if it has an element in common with one of the early cosets a_1*H … a_k*H. If so, then $b_{k+1}*H$ is equal to the coset it has an element in common with. So toss $b_{k+1}*H$ out. Once we toss out all the duplicates, we're left with G as the disjoint union of the remaining cosets

$$G=(a_1*H)\cup\ldots\cup(a_s*H)$$

The previous proposition tells us that every coset in the disjoint union has the same number of elements, namely *m*, the number of elements in *H*. Thus if *G* has *n* elements and *s* cosets, then *n = ms*.

Corollary. *For every element b of a finite group G, the order of b divides the number of elements of G.*
Proof. If $H=\langle b\rangle$ is the subgroup generated by *b*. The order of *b* is the number of elements of *H*. The corollary then follows from Lagrange's theorem.

Corollary. *Euler's theorem.*
Proof. Let $G=U_m$ the multiplicative group of units of $\mathbb{Z}/m\mathbb{Z}$ and let *a* be any number in U_m. Then the order *d* of $[a]_m$ is the number of elements of the subgroup $\langle a\rangle$ of U_m. Hence *d* divides the number of elements in U_m, namely $\phi(m)$, and $\phi(m)=ds$ for some number *s.* Then $[a]^{\phi(m)}=[a]^{ds}=[1]^s=[1]$; hence the congruence notation $a^{\phi(m)}\equiv 1(mod\, m)$.

In usual terminology the number of elements of a finite group *G* is called the **order** of *G.* Then the order of *H* divides the order of *G*. The number of cosets of *H* in *G* is called the **index** of *H* in *G*.

(order of G) = (order of *H*) × (index of *H* in *G*)

The two notions of order, for an elements and for a group, are compatible.

For abelian groups the left cosets and right cosets are the same. For non-abelian groups this could not be the case.

Fermat's probabilistic primality test

Let U_m be the group of units of $\mathbb{Z}/m\mathbb{Z}$. Then U_m is an abelian group containing $\phi(m)$ elements. Let
$U_m(m-1)=\{[a]\in U_m:\ [a]^{m-1}=[1]\}$
Then $U_m(m-1)$ is the set of units *a* such that *m* passes the ***a-pseudoprime*** test.

Note that for each $[a]$ in U_m, it is only guaranteed that $[a]^{\phi(m)}=[1]$. Obviously we don't generally know how many elements U_m has; if we already know that $|U_m|<m-1$ then *m* would be composite and the primality test is not required.

Proposition. $U_m(m-1)$ *is a subgroup of* U_m.
Proof. Given $[a]$ *and* $[b]$ *in* $U_m(m-1)$. Since $[a]^{m-1}=[b]^{m-1}=[1]$, then $[a]^{m-1}[b]^{m-1}=[ab]^{m-1}=[1]$
Thus $U_m(m-1)$ is closed under the product. Furthermore $[a]^{m-1}$ is its own multiplicative inverse.

Corollary. *If m passes the a-pseudoprime test and the b-pseudoprime test, it passes the ab-pseudoprime test.*

By Fermat's theorem, if *m* is prime then $U_m(m-1)=U_m$. Unfortunately, the converse is not true. If $U_m(m-1)=U_m$ then *m* can be prime or a Carmichael number. But as soon as we find out that $U_m(m-1)\neq U_m$, i.e. *m* doesn't pass an *a-pseudoprime* test, we can assert that *m* is composite.

Proposition. *If m is not prime and not a Carmichael number, then m will pass the a-pseudoprime test for at most half of the numbers a,* $1\leq a\leq m$.
Proof. If $U_m(m-1)\neq U_m$ and f is the number of elements of $U_m(m-1)$ then among the $s=\phi(m)/f$ cosets of $U_m(m-1)$ in U_m only the f elements of $U_m(m-1)$ satisfy $[a]^{m-1}=[1]$, while $(s-1)f$ elements not. Since $U_m(m-1)\neq U_m$, then there are at least two cosets, so $s\geq 2$ and $(s-1)f\geq f$. Thus, since $s\geq 2$, we have that the test will fail for at least half of the elements.

In other words, the probability that *a* is composite and pass *a-pseudoprime* test $\leq$ ½.
If we repeat the test for say 20 randomly chosen a values, then the probability that *m* is composite and passes the all the *a-pseudoprime* tests is less than $1/2^{20}$ or less than one in a million.

Equations

Generalization of equation solving result for any Abelian group.
Given *e* the identity element of *G*, the equation $x^n=e$ is *homogeneous*.

Proposition. *Let G be an abelian group with operation multiplication and identity e.*
Let $G(n)=\{h\in G:\ h^n=e\}$ *be the set of solutions in G of the equation* $x^n=e$. *Given* $c\in G$, *if there is some b in G so that* $b^n=c$, *then the set of solutions to the equation* $x^n=c$ *is the coset* $bG(n)=\{bh:\ h\in G(n)\}$.
Proof. If $b^n=c$, then for all *h* in $G(n)$, $(bh)^n=b^nh^n=c\cdot e=c$. Conversely, if $s^n=c$ for some *s* in *G*, then $(b^{-1}s)^n=b^{-n}s^n=c^{-1}c=e$, so $b^{-1}s=h\in G(n)$. Thus $s=bh$ is in $bG(n)$.

Proposition. *The set of solution of a homogeneous equation is a subgroup of G.*
Proof. Trivial.

Homomorphism

Many concepts of group homomorphism equal to the ones defined for ring's homomorphisms.
Let *G* and *H* be groups with an operation * and identity e_G and e_H, respectively.

Group homomorphism. A function $f: G \to H$ is a group homomorphism if

$f(g_1 * g_2) = f(g_1) * f(g_2)$ for all $g_{1,} g_2 \in G$

$f(e_G) = e_H$

The inverse of $f(g)$ is $f(g)^{-1} = f(g^{-1})$ and is unique.

$e_H = f(e_G) = f(g * g^{-1}) = f(g) * f(g^{-1}) = f(g) * f(g)^{-1}$

Example. If *R* is a ring and we only consider only the operation +, then *R* is an additive group. If $f: R \to S$ is a ring homomorphism, then *f* is a group homomorphism from the additive group of *R* and the additive group of *S*.

Example. If $U(R)$ is the group of units of a ring *R*. If $f: R \to S$ is a ring homomorphism, then if we consider the operation $\cdot$ *f* is a group homomorphism from $U(R)$ to $U(S)$.

Example. If *H* is a subgroup of a group *G*, then the **inclusion map** $i: H \to G$, which takes an element of *H* and views it in *G*, is a group homomorphism.

Example. If *G* is a group, and $f: G \to H$ is a function which takes every element of *G* to the identity element of an arbitrary group *H*, then *f* is a homomorphism, also called the **zero-homomorphism**.

A group homomorphism $f: G \to H$ is one-to-one if it is one-to-one as a function. Or in other words if its kernel is composed by only the identity element.

$ker(f) = \{g \in G: \ f(g) = e\}$

Proposition. *Let $f: G \to H$ be a group homomorphism. Then $ker(f)$ is a subgroup of G.*

Proof. Given $a, b \in ker(f)$, since *f* is a group homomorphism, $f(a * b) = f(a) * f(b) = e_H * e_H = e_H$ then $a * b \in ker(f)$ as well. Also $e_H = f(e_G) = f(a * a^{-1}) = f(a) * f(a^{-1}) = e_H * f(a^{-1}) = f(a^{-1})$, thus $a^{-1} \in ker(f)$. Follows that *H* is a subgroup of *G*.

Proposition. *Let $f: G \to H$ be a group homomorphism. The map f is one-to-one iff $ker(f) = \{e\}$.*

Proof. If $ker(f)\neq\{e\}$ then there is an a in G such that $f(a)=e$, thus is not one-to-one. Conversely, if f is not one-to-one then given $a,b\in G$ such that $a\neq b$ then $f(a)=f(b)$. Assuming both $a,b\neq e_G$ then $a^{-1}\neq e_G$ and $e_H=f(a)^{-1}*f(b)=f(a^{-1}*b)$ with $a^{-1}*b\neq e_H$. Thus $ker(f)\neq\{e\}$.

Definition. Let $f:G\to H$ be a group homomorphism. The **image** of f is the set $f(G)$ of elements of H that have the form $f(g)$ for some $g\in G$.

$$f(G)=\{h\in H:\ h=f(g),\ \text{for some } g\in G\}$$

Proposition. *The image of a group homomorphism $f:G\to H$ is a subgroup of H.*
Proof. Given $f(a),f(b)\in f(G)$. Since f is an homomorphism, $f(a)*f(b)=f(a*b)\in f(G)$. Furthermore $e_H=f(e_G)=f(a*a^{-1})=f(a)*f(a^{-1})$, thus if $f(a)\in G$ then $f(a)^{-1}\in f(G)$.

Isomorphism. A group homomorphism $f:G\to H$ is an *isomorphism* if f is *one-to-one* and *onto*.

Proposition. *If $f:R\to S$ is an isomorphism of rings, then f restricts to an isomorphism $f:U(R)\to U(S)$ from the group of units of R to the group of units of S.*
Proof. If u is a unit of R then $f(u)$ is a unit of S. Suppose t is a unit of S. Let r be the unique element in R so that $f(r)=t$ (r is unique because f is one-to-one) and let r' in R be so that $f(r')=t^{-1}$. Then $f(r*r')=f(r)*f(r')=t*t^{-1}=e_S$. But $f(e_R)=e_S$ and f, being an isomorphism, is one-to-one. Thus $r*r'=e_R$, and r is a unit of R.

Quotient Groups

If G is an abelian group with operation * and H any subgroup, then the left cosets of H in G also form an abelian group, where the operation * on cosets is induced from the operation in G. We denote the group of left cosets of H in G by G/H and is called a **quotient group**.

Example: $\mathbb{Z}$ is an additive group, thus the elements of the congruence classes $\mathbb{Z}/m\mathbb{Z}$ form a group under addition. A more explicit notation for a congruence class $[a]_m\in\mathbb{Z}/m\mathbb{Z}$ is then $a+m\mathbb{Z}$.

Let G be an abelian group with operation *, identity e and H any subgroup. Let G/H be the set of left cosets of H in G. We define an operation on G/H, induced by * in G as $(a*H)*(b*H)=(a*b)*H$.
Before claim that G/H is an abelian group, we want to show that the operation is well-defined.

Proposition. *Suppose* $a*H=a_1*H$ *and* $b*H=b_1*H$ *. Then* $(a*b)*H=(a_1*b_1)*H$.

Proof. It suffices to show that if we pick any element out of the coset $a*H$ and any element out of the coset $b*H$, and multiply them in *G*, we get an element of the coset $(a*b)*H$. Let $a_1=a*h$ and $b_1=b*h$ for some $h,h_1\in H$. If we take the product $a_1*b_1=(a*h)*(b*h_1)$, then since *G* is abelian, we can rearrange the product $(a*h)*(b*h_1)=(a*b)*(h*h_1)$. Since $h*h_1\in H$, the result is in $(a*b)*H$.

Theorem. *If G is an abelian group and H is a subgroup of G, then the set of left cosets G/H is an abelian group, with the operation on cosets induced by the operation on G.*

Proof. Once that we see that * on the cosets is well defined, the group properties follows easily since they hold in *G*. The set $e*H$ is the identity element of G/H , and the inverse of $a*H$ is $a^{-1}*H$ where a^{-1} is the inverse of *a* in *G*.

To show that $\mathbb{Z}/m\mathbb{Z}$ is a group under addition we must prove that the operation + is well-defined. Given two cosets $a+m\mathbb{Z}$ and $b+m\mathbb{Z}$ then the sum has been defined as $a+b+m\mathbb{Z}$.

The Chinese Remainder Theorem

Given two natural numbers *m* and *n* greater than 1 and *a, b* be any integers. Consider the following system of two linear congruences

$\begin{cases} x\equiv a\,(mod\,m) \\ x\equiv b\,(mod\,n) \end{cases}$ equivalent to $\begin{cases} x=a+mz \\ x=b+ny \end{cases}$ for some integers *m, y*

Theorem (existence). *There is a solution* $x=x_0$ *to the system if and only if the greatest common divisor of m and n divides a - b.*

Proof. The system is equivalent to the equation $(b-a)=mz-ny$. Let $d=(m,n)$. ($\rightarrow$) If *d* does not divide $b-a$ then there cannot be integers *z* and *y* satisfying the given equation. ($\leftarrow$) Conversely if *d* divides *a – b* then, using *Bezout's* identity we can find two integers *s* and *t* such that $d=ms+nt$.

Assuming $a-b=qd$, for some integer *q*, we multiply both sides by *q* obtaining $a-b=msq+ntq$. We can then set *z=sq* and *y=-tq*. The solution can be thus derived using the system equations: $x=a+mz=b+ny=a+msq=b-ntq$.

Theorem (form). *If $x=x_0$ is a solution. Then the set of integers x that satisfy the two congruences is the same as the set of x that satisfy $x\equiv x_0 (mod [m,n])$ i.e. $x=x_0+[m,n]k$ where $[m,n]$ is the least common multiple of m and n.*

Proof. ($\rightarrow$) First we show that any solution has that form. Let x_1 be another solution. Then x_1-x_0 is a solution to the homogeneous pair of congruences.

$x_1\equiv a(mod\, m)\wedge x_0\equiv a(mod\, m) \rightarrow x_1-x_0\equiv 0(mod\, m) \rightarrow x_1-x_0=m\,k_1$

$x_1\equiv b(mod\, n)\wedge x_0\equiv b(mod\, n) \rightarrow x_1-x_0\equiv 0(mod\, n) \rightarrow x_1-x_0=n\,k_2$

That means that x_1-x_0 is a common multiple of *m* and *n*, thus by definition is then a common multiple of the least common multiple: $x_1-x_0=[m,n]k$ and thus that $x_1\equiv x_0(mod[m,n])$.

($\leftarrow$) Conversely, we have to show that any number congruent to x_0 modulo $[m,n]$ is a solution.

Let *x* be a number satisfying $x\equiv x_0(mod[m,n])$. Then trivially $x\equiv x_0(mod\, m)$ and $x\equiv x_0(mod\, n)$. And so *x* is also a solution to the original pair of congruences.

In general, given that $x=a+mz=b+ny$, to find *x* we don't need to find both *z* and *y*. We can reduce the calculations by directly solving a single congruence modulo the smaller of the two moduli.

For example: $a+mz\equiv b+ny(mod\, n) \rightarrow mz\equiv(b-a)(mod\, n)$

At this point is sufficient to find m^{-1} modulo *n*, that should be easier than the original problem.

Corollary. *We can express the set of integers that solve a system of two congruences as the set of integers that satisfy a single congruence. Given x_0 a solution to the system: $x\equiv x_0(mod[m,n])$.*

The above corollary allow us to extend the resolution method to systems of three or more congruences.

Corollary. *If m and n are coprime then there is always a solution to the system.*

Chinese Remainder Theorem (existence). *Let $m_1, m_2, \ldots, m_n$ be pairwise coprime natural numbers > 1 and $a_1, a_2, \ldots, a_n$ be arbitrary integers. Then there is a solution to the system:*

$$\begin{cases} x\equiv a_1(mod\, m_1) \\ x\equiv a_2(mod\, m_2) \\ \quad\ldots \\ x\equiv a_n(mod\, m_n) \end{cases}$$

Proof. By induction of *n*. The base case is the one for two congruences and is true for the corollary above. For $n>2$ we assume the theorem true for $n-1$ congruences. We use the corollary for two congrunces to replace the first two congruences by a single congruence: $x \equiv x_0 (mod\, m_1 m_2)$. Then to show that there is a solution to the original set of *n* congruences, we need to show that there is a solution for the set of *n* − 1 congruences consisting of all but the first two of the *n* original congruences, together with the congruence $x \equiv x_0 (mod\, m_1 m_2)$. Observe that $(m_1 m_2, m_j) = 1$ for every $j = 3, \ldots, n$ Thus the set of *n* − 1 congruences has a solution by the induction hypothesis, and the solution is a solution of the original *n* congruences.

Chinese Remainder Theorem (form). *If x_0 is a solution, then the set of integers x that satisfy the system of congruences is the same as the set of x that satisfy* $x \equiv x_0 (mod\, [m_1, m_2, ..., m_n])$

Proof. Extending the lcm to more than two elements, the proof is similar to the theorem for two congruences.

This part of the theorem stress the fact that, given a solution x_0 of the original system, every solution to the original system is a solution of $x \equiv x_0 (mod\, [m_1, m_2, \ldots, m_n])$, and vice-versa.

Alternative resolution method

The idea is to solve a collection of "special" systems and then obtain a solution of the original congruence as a linear combination of the solutions of the special systems.

Example for two congruences:

$$\begin{cases} x \equiv a (mod\, m) \\ x \equiv b (mod\, n) \end{cases}$$

If $(m, n) = 1$ then we known that a solution exists. First we solve the two systems:

$$\begin{cases} x \equiv 1 (mod\, m) \\ x \equiv 0 (mod\, n) \end{cases} \quad \begin{cases} x \equiv 0 (mod\, m) \\ x \equiv 1 (mod\, n) \end{cases}$$

Let e_1 and e_2 be the solutions to the first and the second systems, respectively. Then

$e_1 = 1 + mx_1 = n\, y_1$ and $e_2 = mx_2 = 1 + ny_2$

Making both congruences modulo *m* we obtain $1 \equiv n\, y_1 (mod\, m)$ and $-1 \equiv n\, y_2 (mod\, m)$

Finding the inverse of *n* modulo *m* we find y_1 and consequently e_1.

Similarly, to find y_2 we find the inverse of -*n* modulo *m* (equals to the negative of the inverse of *n*).

Now we can find a solution x_0 to the original system by setting

$$x_0 = a e_1 + b e_2$$

Check: $a e_1 + b e_2 \equiv a \cdot 1 + b \cdot 0 \equiv a \pmod{m}$ and $a e_1 + b e_2 \equiv a \cdot 0 + b \cdot 1 \equiv b \pmod{n}$

The method can be easily extended to be used with systems with more than two congruences.

Tip: in each derived system there is only one congruence with 1 on the right hand side, the others are set congruent to 0. Merge together, in a single congruence, the ones congruent to zero, setting the modulus equal to the least common multiple (lcm).