Number Theory

1) The well ordering principle

- Any non empty set of integers bounded from below has a least element.
- Similarly, any non empty set of integers bounded from above has a greatest element

Consequence: Any finite set of integers has a least and a greatest element.

2) Division

Definition: If a and b are integers, with $a \neq 0$ we say that a divides b if there exists an integer c such that $b = ac$. We say then that a is a factor of b and that b is a multiple of a. The notation $a \mid b$ denotes that a divides b.

Theorem 1 Let a, b, and c be three integers.

1) If a/b and a/c, then $a/(b+c)$
2) If a/b then a/bd for all integers d.
3) If a/b and b/c then a/c
4) If a/b and a/c, then $a/(mb+nc)$ for all integers m and n.

Proofs:

1) Direct proof: Let us suppose a/b and a/c. By definition, there exists two integers m and n such that $b = ma$ and $c = na$. Then $b+c = (m+n)a$ which implies that $a/(b+c)$
2) Direct proof Let us suppose a/b. By definition, there exists an integer m such that $b = ma$. Let d be an integer. $bd = mad = a(md)$, which implies that a/bd.
3) Direct proof. Let us suppose a/b and b/c. There exists two integers m and n such that $b = ma$ and $c = nb$. Therefore $c = nma$, which implies that a divides c.
4) Direct proof. Let m and n be two integers, and let us suppose a/b and a/c. According to (2), $a/(mb)$ and $a/(nc)$. According to 1, $a/(mb+nc)$.

3) Prime numbers

Definition. An integer greater than one is *prime* if its only positive divisors are itself and one.
Otherwise, it is *composite*

4) The fondamental theorem of arithmetics

Every positive integer greater than one can be represented as a product of one or more primes.

Theorem: If n is a composite integer, then n has a prime divisor less than or equal to $\sqrt{n}$.

Proof: Proof by contradiction.
n is composite: there exists a and b integers such that

$$n = a\,b$$

We suppose that $a > \sqrt{n}$ and $b > \sqrt{n}$. Then $ab > n$, which contradicts $n = a\,b$. Therefore $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$.

This leads to a method for finding all prime numbers that are smaller than a given value N

→ sieve of Eratosthenes.

To find all prime numbers that are less than some number N, just consider every number between 2 and $\lfloor \sqrt{n} \rfloor$, and eliminate all their multiples. Those numbers that remain between 2 and N will be prime.

Algorithm:

```
For [i = 2; i ≤ N; Step = 1]
|     Label(i) ← i
]
For [i = 2; i ≤ ⌊√n⌋; Step = 1]
|     if (Label(i) ≠ 0) then
      [
            j = 2
            while (j * Label(i) ≤ N)
                  Label[j * Label(i)] ← 0
                  j ← j + 1
      }
]
```

Theorem: After running the procedure above, the elements with labels that are not 0 are prime.

Proof by case:

1) If p is prime then $Label(p) \neq 0$.

Indirect proof: If $label(p) = 0$, then p is in the form $j * label(i)$ with $j \geq 2$ and $i \geq 2$. Therefore p is not prime.

2) If p is composite, then label$(p) = 0$

Direct proof: Let p be composite. There exists a and b such that $p = a\,b$, and a prime and $a < \sqrt{n}$

a is prime therefore label$(a) \neq 0$. All multiples of a will have their labels set to 0 $\rightarrow$ label$(p) = 0$.

5) The division algorithm

Theorem: Let a ~~and~~ be an integer and d a positive integer. There exists unique integers q and r, with $0 \leq r < d$ such that

$$a = dq + r$$

d: divisor
a: dividend
q: quotient
r: remainder.

$q = a \operatorname{div} d$

$r = a \pmod d$

$(r \equiv a \ [d])$

6) Greatest common divisor

Definition: Let a and b be integers, not both zero. The largest integer d such that $d \mid a$ and $d \mid b$ is called the greatest common divisor of a and b, and is denoted $\gcd(a, b)$

Definition Two integers a and b are said to be relatively prime if $\gcd(a,b)=1$.

Theorem (Bezout's identity) If a and b are two integers that are not both zero, then there exists two integers m and n such that

$$am + bn = \gcd(a,b)$$

1) ~~Least~~ common multiplier

Definition Let a and b be integers, not both zeros. The smallest integer m such that $a|m$ and $b|m$ is called the least common multiple of a and b, and is denoted $\text{lcm}(a,b)$

Theorem: Let a and b be positive integers.

Then: $\gcd(a,b) \times \text{lcm}(a,b) = ab$

Proof We will show that $ab \leq \gcd(a,b) \times \text{lcm}(a,b)$ and $\gcd(a,b) \times \text{lcm}(a,b) \leq ab$.

1) Let a and b be non zero integers. According to Bezout's identity, there exists two integers m and n such that $\gcd(a,b) = am + bn$

After multiplication with $\text{lcm}(a,b)$:

$\text{lcm}(a,b)\,\gcd(a,b) = \text{lcm}(a,b)\,am + \text{lcm}(a,b)\,bn$

$\text{lcm}(a,b)$ is a multiple of both a and b: there exists two integers k and l such that

$\text{lcm}(a,b) = ka$ and $\text{lcm}(a,b) = lb$.

Therefore: $\text{lcm}(a,b)\gcd(a,b) = lbam + kabn$

$= ab(lm + kn)$

Therefore: ab is a divisor of $\text{lcm}(a,b)\gcd(a,b)$

We can conclude: $ab \leq \text{lcm}(a,b)\gcd(a,b)$

2) $\gcd(a,b)$ is a divisor of both a and b: there exists two integers v and e such that $a = \gcd(a,b)\,v$ and $b = \gcd(a,b)\,e$

Therefore: $ab = \gcd(a,b)\,v\,b$ (a)

and $ab = \gcd(a,b)\,e\,a$ (b)

$\gcd(a,b)$ is a divisor of ab: there exists t integer such that $ab = t\gcd(a,b)$

Then (a) becomes $t\gcd(a,b) = \gcd(a,b)\,vb$

i.e $t = vb$

and (b) becomes $t\gcd(a,b) = \gcd(a,b)\,ea$

i.e $t = ea$

E is a common multiple of a and b; since $\text{lcm}(a,b)$ is the smallest, $\text{lcm}(a,b) \leq t$

After multiplying with $\gcd(a,b)$: $\gcd(a,b)\,\text{lcm}(a,b) \leq t\gcd(a,b)$

i.e $\gcd(a,b)\,\text{lcm}(a,b) \leq ab$. This concludes the proof.

8) Modular arithmetic

Definition: Let a and b be two integers and m be a positive integer. a is said to be congruent to b modulo m if m divides $a-b$. We use the notations:

$$a \equiv b \pmod{m}$$

or $$a \equiv b \ [m]$$

or $$a \equiv_m b.$$

Theorem: Let a and b be integers, and let m be a positive integer. Then $a \equiv b \ [m]$ if and only if $a \bmod m = b \bmod m$ (i.e. the remainders of the divisions of a by m and b by m are equal).

Proof: We need to prove a biconditional (if and only if) which we prove by proving both implications.

a) We prove that If $a \equiv b \ [m]$ then $a \bmod m = b \bmod m$.

By definition, $a \equiv b \ [m]$ means $m \mid a-b$.
Therefore there exists an integer k such that $a-b = km$
Let us divide a and b by m:
There exists unique q and r such that $a = mq + r$.
Similarly, there exists unique s and t such that $b = ms + t$

$$a - b = m(q-s) + r - t$$

Therefore: $m(k-q+r) = r-t$

m divides $r-t$, but $-m < r-t < m$. This is only possible if $r-t=0$, i.e $r=t$ or $a \bmod m = b \bmod m$.

b) We prove that if $a \bmod m = b \bmod m$, the $a \equiv b \ [m]$.

Again, we divide a and b by m:

$a = mq + r$

$b = ms + t$

We know that $t = r$, therefore $b = ms + r$

Then $a - b = m(q-s)$, i.e $m \mid (a-b)$

By definition, $a \equiv b \ [m]$.

This concludes the proof.

Theorem: Let m be a positive integer.

If $a \equiv b \ [m]$ and $c \equiv d \ [m]$ then

$a + c \equiv b + d \ [m]$ and $ac \equiv bd \ [m]$

Proof: (a) $a \equiv b \ [m]$ implies $m \mid (a-b)$

$c \equiv d \ [m]$ implies $m \mid (c-d)$

Based on theorem 1 on division, $m \mid (a-b)+(c-d)$

i.e $m \mid (a+c) - (b+d)$, i.e $a+c \equiv b+d \ [m]$

(b) $m \mid (a-b)$ therefore $m \mid c(a-b)$ i.e $m \mid (ac - bc)$

$m \mid (c-d)$ therefore $m \mid b(c-d))$ i.e $m \mid bc - bd$

then $m \mid ac - bd$ i.e $ac \equiv bd \ [m]$

Theorem: If p is a prime number and a is a natural number, then:

$$a^p \equiv a \ [p]$$

or

$$a^{p-1} \equiv 1 \ [p]$$

This is called Fermat's little theorem.

This theorem is often used as a "proof of primality":

If n verifies $2^n \equiv 2 \ [n]$, it is probably prime.

If $2^n \not\equiv 2 \ [n]$, n is composite.

If $2^n \equiv 2 \ [n]$, n is called a weak probable prime.

Only one "mistake" for n below < 500!

$n = 341$ satisfies $2^{341} \equiv 2 \ [341]$, but 341 is not prime.

Proof of Fermat's little theorem.

We first show that:

Theorem: if p is prime, and p does not divide a, then $a^{p-1} \equiv 1 \ [p]$

Let us consider the first $(p-1)$ multiples of a:

$a, 2a, \ldots ia, \ldots (p-1)a$.

Let us write:

$$a \equiv k_1 \pmod p \quad 0 < k_1 < p$$
$$\vdots$$
$$ia \equiv k_i \pmod p \quad !$$
$$\vdots$$
$$(p-1)a \equiv k_{p-1} \pmod p \quad 0 < k_{p-1} < p$$

Lemma: All $(k_i)_{i=1,p-1}$ are distincts.

Indirect proof: Suppose there exists i and j such that $k_i = k_j$

Then $ia \equiv ja \pmod p$

$p \mid (i-j)a$

p is prime. Then $p \mid (i-j)$ or $p \mid a$

No since $i-j < p$ — No by hypothesis

We reach a contradiction: the Lemma is true.

Since all $|k_i|_{i=1,p-1}$ are different, and they are all (10
smaller than $(p-1)$, $S=[k_1,\dots k_{p-1}]$ is a
rearrangement of $[1,\dots,p-1]$.

Since $a \equiv k_1 \ [p]$

$\vdots$

$(p-1)a \equiv k_{p-1} \ [p]$

$a \times 2a \times \dots (p-1)a \equiv k_1 \times \dots \times k_{p-1} \ [p]$

$a^{p-1}(p-1)! \equiv (p-1)! \ [p]$

Lemma 2 : If p is prime, p does not divide c and $ac \equiv bc \ [p]$, then

$a \equiv b \ [p]$

Proof: If $ac \equiv bc \ [p]$ then $p \mid (a-b)c$
Since p is prime, $p \mid (a-b)$ or $p \mid c$.
by hypothesis, $p \nmid c$ then $p \mid (a-b)$ Hence $a \equiv b [p]$

Using lemma 2, since p does not divide $(p-1)!$,

$x^{p-1} \equiv 1 \ [p]$ ∎

Let us now consider p prime, and a integer.
If $p \mid a$, $a^p \equiv 0 \ [p]$ and $a \equiv 0 \ [p]$, hence $a^p \equiv a \ [p]$
If $p \nmid a$, $a^{p-1} \equiv 1 \ [p]$ then $a^p \equiv a \ [p]$.

9) Some important results from Euclid

Proposition 1 If p is a prime number and p/ab, Then p/a or p/b

Proof: We use a ~~direct~~ proof by contradiction.

Let p be a prime number such that p/ab.

Suppose p does not divide a and b. Then $\gcd(p,a)=1$.

According to Bezout's identity, there exists u and v such that $pu+av=1$. (a)

Since p/ab, there exists an integer k such that $ab=kp$.

We multiply (a) by b:

$$pub+abv=b$$

Then $$pub+kpv=b$$

Hence $$p(ub+kv)=b$$

p/b but the hypothesis was $p \nmid b$. We have reached a contradiction. Proposition 1 is true.

Proposition 2: There is an infinite number of prime numbers.

Proof by contradiction Let us suppose the number of prime number is finite: N

$$S = [p_1, \dots, p_N]$$

Let us define $P = p_1 \times p_2 \times \dots \times p_N + 1$

None of the p_i divide P (otherwise they would divide 1). However, according to the fundamental theorem of arithmetics, every integer N can be written as a finite product of prime factors. Any of these prime factors for the integer P would be a new prime number, which contradicts the hypothesis. Hence proposition 2 is true.

Euclid's algorithm for computing gcd(a,b)

Euclid noticed that:

(1) If $b = a$, then $\gcd(a,b) = a$

(2) $\forall (a,b) \in \mathbb{N}^2$, if $b > a$, then $\gcd(a,b) = \gcd(a, b-a)$

Proof:

(1) is trivial

(2) Let $g = gcd(a, b)$ and $h = gcd(a, b-a)$ for two integers a, b with $b > a$.

Since g divides a and g divides b, ~~there exists~~ g divides $(a-b)$. Hence g is a divisor of $b-a$, and a, and since h is the greatest, $g \leq h$.

Reciprocity.

Since h divides a and h divides $(b-a)$, h divides $(b-a)+a$, i.e h divides b. Therefore h is a divisor of a and b, and since g is the greatest, $h \leq g$.

Therefore $gcd(a, b) = gcd(a, b-a)$

This suggests an algorithm for computing the gcd of two numbers:

Replace the largest number with the difference of the 2 numbers, until the 2 numbers are equal, in which case the gcd is equal to any of the number.

```
Procedure gcd-Euclid (a: int, b: int)
while (a ≠ b)
{
    if (a > b) then
        a ← a - b
    else
        b ← b - a
    endif
}
gcd (a, b) = a.
```

Complexity?

The wast case corresponds to a (or b) = 1, in which case the number of steps is b (or a).

Note that if a = 1, gcd (a, b) = 1.

A faster variant:

Based on 2 observations:

(1) If b | a, then gcd (a, b) = b

(2) If a = bq + r, gcd (a, b) = gcd (b, r)

Proofs:

(1) gcd (a, b) ≤ b by definition of gcd.

Since b | a and b | b, b is a divisor of a and b.

As gcd (a, b) is the greatest common divisor,

b ≤ gcd (a, b)

Therefore gcd (a, b) = b

(2) We know:

- $gcd(a,b) \mid a$
- $gcd(a,b) \mid b$ then $gcd(a,b) \mid bq$

Therefore $gcd(a,b) \mid a-bq$, i.e. $gcd(a,b) \mid r$

$gcd(a,b)$ is a common divisor of b and r,

Therefore $gcd(a,b) \leq gcd(b,r)$

Reciprocity

$gcd(b,r) \mid b$ Therefore $gcd(b,r) \mid bq$

$gcd(b,r) \mid r$

Therefore $gcd(b,r) \mid (bq+r)$, i.e. $gcd(b,r) \mid a$.

$gcd(b,r)$ is therefore a common divisor of a and b,

therefore $gcd(b,r) \leq gcd(a,b)$.

This suggests a method to compute $gcd(a,b)$:

$$
\begin{aligned}
a &= b\,q_1 + r_1 && gcd(a,b) \\
b &= r_1\,q_2 + r_2 && = gcd(b,r_1) \\
r_1 &= r_2\,q_3 + r_3 && = gcd(r_1,r_2) \\
r_2 &= r_3\,q_4 + r_4 && = gcd(r_2,r_3) \\
&\vdots \\
r_{n-1} &= r_n\,q_{n+1} + r_{n+1} && = gcd(r_{n-1},r_n) \\
r_n &= r_{n+1}\,q_{n+2} + 0 && = gcd(r_n,r_{n+1}) \\
& && = r_{n+1}
\end{aligned}
$$

We are sure that the procedure stops, as the successive r_n are strictly decreasing and positive.

In pseudo code:

```
Procedure gcd-Euclid2 (a: int>0, b: int>0)
    Integer t
    while (b ≠ 0)
    {
        t ← b
        b ← a (mod b)
        a ← t
    }
    gcd (a, b) = b
```