BASIC NUMBER THEORY

DIRK KUSSIN

Essentially the same material can be found also in Chapter 3 of the textbook [1].

1. Divisiblity

Number theory is concerned with the properties of the integers.

Definition 1.1. Let a and b integers with $b \neq 0$. We say that b *divides* a if there is an integer c such that $a = bc$. In this case we write $b \mid a$. One also says that a is a *multiple* of b.

Examples: $3 \mid 15$, since $15 = 3 \cdot 5$. $7 \nmid 18$ (does not divide).

Proposition 1.2. *Let a, b, $c \in \mathbb{Z}$.*

(1) *For every $a \neq 0$ we have $a \mid 0$ and $a \mid a$. For every b we have $1 \mid b$.*
(2) *If $a \mid b$ and $b \mid c$ then $a \mid c$.*
(3) *If $a \mid b$ and $a \mid c$ then $a \mid (sb + tc)$ for all integers s and t.*

Proof. [...] □

2. Congruences

Definition 2.1. Let $n \neq 0$ be an integer. For a, $b \in \mathbb{Z}$ we write

$$a \equiv b \mod n$$

(or just $a \equiv b$ if it is clear that it is taken modulo n) (read: a is *congruent* to b *mod* n), if $a - b$ is divisible by n.

Proposition 2.2. *Let a, b, c, $n \in \mathbb{Z}$ with $n \neq 0$.*

(1) $a \equiv 0 \mod n$ *if and only if* $n \mid a$.
(2) $a \equiv a \mod n$.
(3) $a \equiv b \mod n$ *if and only if* $b \equiv a \mod n$.
(4) *If* $a \equiv b \mod n$ *and* $b \equiv c \mod n$ *then* $a \equiv c \mod n$.

The last three conditions precisely mean that $\equiv$ is an equivalence relation on the set of integers.

Proof. [...] □

Date: November 12, 2007.

Proposition 2.3. *Let $n \neq 0$ be a positive integer, and let $a \in \mathbb{Z}$. Then there are* unique *integers q and r such that*

$$a = nq + r \quad \text{and } \textit{with} \quad 0 \leq r < n.$$

Proof. There is an integer q such that $qn \leq a$ and such that $(q{+}1)n > a$. Define $r \overset{def}{=} a - nq$. Then $a = qn + r$ and $0 \leq r < n$. If also $a = q'n + r'$ with $0 \leq r' < n$ then $r - r' = (q' - q)n$, and since $|r - r'| < n$, only $r - r' = 0$ and $q - q' = 0$ is possible, that is, $r = r'$ and $q = q'$. □

Since, in particular, r is uniquely determined by a and n, we can write

$$a \bmod n \overset{def}{=} r.$$

Note that always $a \bmod n \in \{0, 1, \ldots, n-1\} \overset{def}{=} \mathbb{Z}_n$.

Lemma 2.4. *Let a and b be integers and n a nonzero integer. Then we have $a \bmod n = b \bmod n$ if and only if $a \equiv b \mod n$.*

Proof. Let $a = qn + r$ and $b = pn + s$ with $0 \leq r,\, s < n$. Then, by definition, $r = a \bmod n$ and $s = b \bmod n$. If $r = s$, then $a - b = (q - p)n$ is a multiple of n, hence $a \equiv b \mod n$. Conversely, if $a \equiv b \mod n$, then there is an integer k with $a - b = kn$. But $a - b = (q - p)n + (r - s)$. It follows that $r - s$ is a multiple of n. On the other hand, $|r - s| < n$, hence $r - s = 0$, that is, $r = s$. □

Proposition 2.5. *Let $n \neq 0$ be an integer. For all integers a, b, c and d we have the following: If $a \equiv b \mod n$ and $c \equiv d \mod n$ then*

$$a + c \equiv b + d \mod n, \quad a - c \equiv b - d \mod n \quad \textit{and} \quad ac \equiv bd \mod n.$$

Proof. Write $a = b + nk$ and $c = d + n\ell$ with integers k and ℓ. Then $a + c = b + d + n(k + \ell)$. Moreover, $ac = bd + n(dk + b\ell + nk\ell)$. □

What is missing here is the division. We need it for studying the so-called affine ciphers. This is a variation of the shift cipher: We again shift but additionally multiply.

The shift cipher is a map $\mathbb{Z}_n \longrightarrow \mathbb{Z}_n$, $x \mapsto x + t \bmod n$ (where $n = 26$ in the example). This is a bijevtive map, the inverse map obviously given by $y \mapsto y - t \bmod n$. We need a bijective map in order to be able to decrypt and get back the plaintext from the ciphertext in a unique way.

The affine cipher is a map

$$\begin{aligned} &\mathbb{Z}_n \longrightarrow \mathbb{Z}_n \\ &x \mapsto ax + b \bmod n \end{aligned}$$

where a is nonzero. But what about bijectivity? If $y = ax + b$, then we have to solve $x = \frac{1}{a}(y - b) \bmod n$. For example, if $n = 26$ and $a = 9$, $b = 2$, then we have to solve $x = \frac{1}{9}(y - 2) \bmod 26$, and we have to find a multiplicative inverse of 9 modulo 26. In fact, this is possible. One finds $9 \cdot 3 = 27 \equiv 1 \mod 26$, thus $y = 3(y-2) = 3y-6 \equiv 3y+20 \mod 26$ is the solution.

Let's try another example, say $a = 13$, $b = 4$. Then the plaintext `input` is mapped to `ERRER` (exercise). We already see, different letters are mapped to the same letter. Or more drastically. The plaintext `alter` gives the same ciphertext `ERRER`. This means, that the the ciphertext `ERRER` cannot be decrypted in a unique way. So we need an additional assumption such that this works. This will lead to the condition that a and n are coprime, that is, that there greatest common divisor is 1.

3. Greatest common divisor

Definition 3.1. Let a and b be integers. An integer d is called a *greatest common divisor* of a and b ($d = \gcd(a, b)$) if the following holds:

1. d is a divisor of both a and b ("common divisor");
2. if d' is an integer which also divides a and b, then $d' \mid d$. ("greatest");
3. $d \geq 0$.

a and b are said to be *coprime* if 1 is a gcd of a and b.

Proposition 3.2. *Let a and b two integers. Then $d = \gcd(a, b)$ exists and is unique.*

Proof. We first show **uniqueness**: Assume that d and d' are two greatesr common divisors of a and b. By the second condition of a gcd we have $d' \mid d$, and $d \mid d'$. Hence there are integers k and ℓ such that $d = kd'$ and $d' = \ell d$. Hence $d = k\ell d$. Either $d = 0$ (and then also $d' = 0$, hence $d' = d$) or $d \neq 0$. Cancelation of d gives $k\ell = 1$. Since k and ℓ are integers, we get k, $\ell = \pm 1$, hence $d' = \pm d$. Since d, $d' \geq 0$ we get $d' = d$.

We show **existence**: Let us first treat special cases: If $a = 0 = b$, then 0 is obviously a gcd. If $a \neq 0$, and $b = 0$, then a is obviously a gcd. (Both cases are not interesting for us in the future. Also, replacing a by $-a$, or b by $-b$, or both, does not change the gcd. We can therefore assume that both a, $b > 0$. Without loss of generality we can assume $a > b$. We then apply divison with remainder:

$$a = qb + r \quad \text{with} \quad 0 \leq r < b.$$

Now, if d is a gcd for b and r, then it is also a gcd for a and b (and conversely): Since d divides b and r_1, it divides also $a = q_1 b + r_1$. If d' divides also a and b, then ist divides also $r_1 = a - q_1 b$, thus $d' \mid d$.

Now we continue: Write

$$b = q_2 r + r_2, \quad \text{mit} \quad 0 \leq r_2 < r_1$$

and so on. Since in this way $r_i < r_{i-1} < \cdots < r_2 < r_1 < b$, there must be a step k where $r_k > 0$ but $r_k + 1 = 0$, that is,

$$r_{k-1} = q_{k+1} r_k + 0.$$

We have shown above that $\gcd(r_{k-1}, r_k) = \gcd(r_k, 0) = r_k$ (and for r_k and 0 the gcd really exists!), and inductively we see that the gcd of a and b exists and is given by r_k. □

Note, that our existence proof actually provides an algorithm for calculating the gcd. This algorithm is called the **Euclidean algorithm**.

Example 3.3. Compute $\gcd(482, 1180)$:

$$\begin{aligned} 1180 &= 2 \cdot 482 + 216 \\ 482 &= 2 \cdot 216 + 50 \\ 216 &= 4 \cdot 50 + 16 \\ 50 &= 3 \cdot 16 + 2 \\ 16 &= 8 \cdot 2 + 0 \end{aligned}$$

We conclude $\gcd(1180, 482) = 2$.

Theorem 3.4. *Let a and b integers, at least one of them nonzero. Let $d = \gcd(a, b)$. Then there are integers x and y such that $d = ax + by$.*

Proof. In order to proof existence of the gcd and to compute $d = \gcd(a, b)$ we used the Euclidean algorithm, that is, applied a finite number of divisions with remainder; we only made use of the remainders r_1, $r_2, \ldots$, $r_k = d$, but not of the quotients. We will, step by step, write $r_i = ax_i + by_i$, so that finally $d = r_k = ax_k + by_k$. We have $a = q_1 b + r_1$. Then $r_1 = a \cdot 1 + b \cdot (-q_1)$. So let $x_1 = 1$ and $y_1 = -q_1$. In the next step, $b = q_2 r_1 + r_2$, and hence $r_2 = b - q_2 r_1 = b - q_2(a - bq_1) = a(-q_2) + b(1 - q_1)$. So let $x_2 = -q_2$ and $y_2 = 1 - q_1$. Assume that x_i, x_{i+1} and y_i, y_{i+1} are already calculated so that

$$r_i = ax_i + by_i$$
$$r_{i+1} = ax_{i+1} + by_{i+1}.$$

The next step in the Euclidean algorithm gives $r_i = q_{i+1} r_{i+1} + r_{i+2}$. Hence

$$\begin{aligned} r_{i+2} &= r_i - q_{i+1} r_{i+1} \\ &= ax_i + by_i - q_{i+1}(ax_{i+1} + by_{i+1}) \\ &= a(x_i - q_{i+1} x_{i+1}) + b(y_i - q_{i+1} y_{i+1}), \end{aligned}$$

hence let $x_{i+2} = x_i - q_{i+1} x_{i+1}$ and $y_{i+2} = y_i - q_{i+1} y_{i+1}$. Then $r_{i+2} = ax_{i+2} + by_{i+2}$. □

The preceding proof provides an algorithm to compute $d = \gcd(a, b)$ *and* additionally integers x and y such that $d = ax + by$. This is called the **extended Euclidean algorithm**.

Example 3.5. Let $a = 60972$ and $b = 19404$. Use the extended Euclidean algorithm as shown in the following schematic way (see next table).

					60972	$=$	$1 \cdot 60972$	$+$	$0 \cdot 19404$
					19404	$=$	$0 \cdot 60972$	$+$	$1 \cdot 19404$
60972	$=$	$3 \cdot 19404$	$+$	2760	2760	$=$	$1 \cdot 60972$	$+$	$-3 \cdot 19404$
19404	$=$	$7 \cdot 2760$	$+$	84	84	$=$	$-7 \cdot 60972$	$+$	$22 \cdot 19404$
2760	$=$	$32 \cdot 84$	$+$	72	72	$=$	$225 \cdot 60972$	$+$	$-707 \cdot 19404$
84	$=$	$1 \cdot 72$	$+$	12	12	$=$	$-232 \cdot 60972$	$+$	$729 \cdot 19404$
72	$=$	$6 \cdot 12$	$+$	0					

4. Congruences and division

Proposition 4.1. *Let a, b, c be integers, and n a nonzero integer. Assume that* $\gcd(a,n) = 1$. *Then*

$$ab \equiv ac \mod n \quad \Rightarrow \quad b \equiv c \mod n.$$

Proof. By the preceding theorem, there are integers x and y such that

$$1 = ax + ny.$$

Multiplying this equation by $b - c$ on both sides gives

$$b - c = (ab - ac)x + n(b - c)y.$$

$ab \equiv ac \mod n$ means that $ab - ac$ is a multiple of n. Since $n(b-c)y$ is also a multiple of n, this is also true for the $b - c$, which means $b \equiv c \mod n$. □

Corollary 4.2. *Assume that* $\gcd(a,n) = 1$. *Then there is an integer b such that $ab \equiv 1 \mod n$. The converse is also true.*

b is a multiplicative inverse of a modulo n.

Proof. If $\gcd(a,n) = 1$, then there are integers x and y such that

$$1 = ax + ny.$$

Define $b = x$. Then $ab = 1 - ny \equiv 1 \mod n$.

Assume conversely, that there is an integer b with $ab \equiv 1 \mod n$. Then there is also an integer y such that $1 = ab + ny$. If d is a common divisor of a and n, then $d \mid 1$ follows from this equation, and hence $\gcd(a,n) = 1$. □

Remark 4.3. In case $\gcd(a,n) = 1$ a multiplicative inverse of a modulo n is computed via the extended Euclidean algorithm. (Example in the exercises.)

Corollary 4.4. *Let a, b and n be integers, a and n nonzero, and such that* $\gcd(a,n)=1$. *Then the map*

$$f: \begin{array}{c} \mathbb{Z}_n \longrightarrow \mathbb{Z}_n \\ x \mapsto ax + b \bmod n \end{array}$$

is bijective.

Proof. Let a' the multiplicative inverse of a modulo n, that is, with $aa' \equiv 1 \mod n$. Consider the map

$$g: \begin{array}{c} \mathbb{Z}_n \longrightarrow \mathbb{Z}_n \\ y \mapsto a'(y-b) \bmod n \end{array}$$

For all $x \in \mathbb{Z}_n$ we have

$$\begin{aligned} (g \circ f)(x) &= g(f(x)) \equiv g(ax+b) \equiv a'(ax+b-b) \\ &= a'(ax) = (a'a)x \equiv x \mod n \\ &= x. \end{aligned}$$

Also, for all $y \in \mathbb{Z}_n$ we have

$$\begin{aligned} (f \circ g)(y) &= f(g(y)) \equiv f(a'(y-b)) \equiv aa'(y-b)+b \\ &\equiv y-b+b = y \bmod n \\ &= y. \end{aligned}$$

We have shown, that g is the inverse map of f, hence f is bijective.

An alternative proof is to show that f is injective and surjective. f is injective: Let x, $y \in \mathbb{Z}_n$ such that $f(x) = f(y)$. This means $ax + b \bmod n = ay + b \bmod n$, hence $ax + b \equiv ay + b \mod n$, hence $ax \equiv ay \mod n$. Since $\gcd(a,n) = 1$ we have $x \equiv y \mod n$. We conclude $x = y$ (since both are in $\mathbb{Z}_n$). Hence f is injective. Now f maps the finite set $\mathbb{Z}_n$ into itself, one-to-one, and hence it is also surjective. □

Exercise: Show that if (a and n nonzero and) $\gcd(a,n) \neq 1$ then the above map is *never* injective.

5. Modular exponentation

In the RSA algorithm we have to calculate powers of the form

$$x^e \bmod n.$$

Suppose we want to compute $6^{1031} \bmod 789$. First computing 6^{1031} and then reducing modulo 789 would produce huge numbers. Instead we multiply step by step and reduce modulo 789 in between, performing divisions with remainder. We use the method of so-called repeated squaring.

Write 1031 as a sum of powers of 2:

$$1031 = 1024 + 4 + 2 + 1 = 2^{10} + 2^2 + 2^1 + 2^0.$$

We then compute $6^2 = 36$,

$$\begin{array}{rclclcrl}
6^4 & = & 36^2 & = & 1296 & \equiv & 507 & \bmod 789 \\
6^8 & = & 507^2 & = & 257049 & \equiv & 624 & \bmod 789 \\
6^{16} & = & 624^2 & = & 389376 & \equiv & 399 & \bmod 789 \\
6^{32} & \equiv & 399^2 & = & 159201 & \equiv & 612 & \bmod 789 \\
6^{64} & \equiv & 612^2 & = & 374544 & \equiv & 558 & \bmod 789 \\
6^{128} & \equiv & 558^2 & = & 311364 & \equiv & 498 & \bmod 789 \\
6^{256} & \equiv & 498^2 & = & 248004 & \equiv & 258 & \bmod 789 \\
6^{512} & \equiv & 258^2 & = & 66564 & \equiv & 288 & \bmod 789 \\
6^{1024} & \equiv & 288^2 & = & 82944 & \equiv & 99 & \bmod 789
\end{array}$$

Now we see $6^{1031} = 6^{1024} \cdot 6^4 \cdot 6^2 \cdot 6^1 \equiv 99 \cdot 507 \cdot 36 \cdot 6 \equiv \boxed{39} \bmod 789$. For a general algorithmic version of this see the textbook [1], Exercise 23 in Chapter 3.

6. The chinese remainder theorem

Theorem 6.1. *Suppose* $\gcd(m, n) = 1$. *For every pair of integers* a *and* b *there is precisely one solution* $x \in \mathbb{Z}_{mn}$ *for the simultaneous congruences*

$$\begin{aligned} x &\equiv a \bmod m \\ x &\equiv b \bmod n. \end{aligned}$$

Proof. Since $\gcd(m, n) = 1$ there are integers s and t such that

$$1 = ms + nt.$$

Then $ms \equiv 1 \bmod n$ and $nt \equiv 1 \bmod m$. Let

$$x \overset{def}{=} bms + ant.$$

Then $x \equiv ant \equiv a \bmod m$ and $x \equiv bms \equiv b \bmod n$. Hence a solution exists. If y is another one, then $y \equiv x \bmod m$ and $y \equiv x \bmod n$. So $y \equiv x \bmod mn$, which follows from the following lemma. □

Lemma 6.2. *Assume* $\gcd(m, n) = 1$. *If* a *is an integer such that* $m \mid a$ *and* $n \mid a$, *then* $mn \mid a$.

Proof. There are integers x and y such that $1 = mx + ny$. Moreover, $a = a'm$ and $a = a''n$, for suitable a' and a''. Multiplying the first equation by a we get $a = a''xmn + a'ymn = (a''x + a'y)mn$, hence a is divisible by mn. □

Example 6.3. Since $\gcd(12, 25) = 1$, the following system of congruence relations is solvable.

$$\begin{aligned} x &\equiv 2 \bmod 12 \\ x &\equiv 4 \bmod 25. \end{aligned}$$

We see (or compute with the extended Euclidean algorithm) $1 = (-2) \cdot 12 + 1 \cdot 25$. The proof shows that

$$x = 4 \cdot (-2) \cdot 12 + 1 \cdot 2 \cdot 25 = -46,$$

and then also $254 = -46 + 12 \cdot 25$ is a solution of the system.

Theorem 6.4 (Chinese Remainder Theorem). *Let $m_1, m_2, \dots, m_s$ be integers which are pairwise coprime, that is,* $\gcd(m_i, m_j) = 1$ *for all* $1 \leq i, j \leq s$ *with $i \neq j$. Given any integers $a_1, a_2, \dots, a_s$ there is precisely one solution x modulo $m_1 m_2 \dots m_s$ to the simultaneous congruences*

$$\begin{aligned} x &\equiv a_1 \bmod m_1 \\ x &\equiv a_2 \bmod m_2 \\ &\cdots \\ x &\equiv a_s \bmod m_s. \end{aligned}$$

7. Prime numbers

Definition 7.1. An integer $p > 1$ is called *prime*, if it is only divisible by 1 and itself, that is, if $p = ab$ with postive integers a and b, then $a = 1$ and $b = p$, or $a = p$ and $b = 1$.

Lemma 7.2 (Euclid's Lemma). *Let $p > 1$ be an integer. Then p is prime if and only if for all integers a and b we have:*

$$p \mid ab \quad \Rightarrow \quad p \mid a \text{ or } p \mid b. \tag{1}$$

Proof. If (1) holds for all integers a and b, then clearly p is prime: If $p = ab$, then $p \mid ab$, hence $p \mid a$ or $p \mid b$, but a and b are also divisors of p.

Assume, p is prime, and let a and b integers such that $p \mid ab$. Assume that $p \nmid a$. We have to show that then $p \mid b$. Since $p \nmid a$ we have $\gcd(p, a) = 1$. Thus there are integers x and y such that

$$1 = px + ay.$$

Multiplying with b we get

$$b = pbx + aby,$$

and since $p \mid ab$ the right hand side is divisible by p, hence also the left hand side, that is, $p \mid b$. □

By induction it follows: Divides a prime p a product of m integers ($m \geq 1$), $p \mid a_1 a_2 \dots a_m$, then there is (at least) one i such that $p \mid a_i$.

The next theorem, also called the fundamental theorem of arithmetic, shows that the prime numbers are the building blocks, the *atoms* of the integers.

Theorem 7.3. *Every positive integer n is a product of primes,*

$$n = p_1 p_2 \dots p_r.$$

This factorization is unique, up to reordering the factors.

Convention: 1 is the empty product: $1 = \prod_{i=1}^{0} p_i$.

Proof. Existence. Proof by induction. $n = 1$ is the empty product (by convention). Let $n > 1$. Either n is prime (and then it is of course a product of primes), or it is not prime. In the latter case we can write $n = ab$, with $1 < a$, $b < n$. By induction now a and b are products of prime numbers, hence is there product $n = ab$.

Uniqueness. Assume that $n = p_1 \dots p_r = q_1 \dots q_s$, where all p_i and all q_j are prime numbers. We have to show that $r = 2$ and up to some reordering $p_i = q_i$ for all $i = 1, \dots, r$. If $r = 0$ (empty product), then $n = 1$, and also $s = 0$ follows, and the statement is clear. Hence let us assume that $r > 0$. Then p_r is a divisor of the product $q_1 \dots q_s$, hence it divides one of them, say $p_r \mid q_j$. By reordering we can assume $p_r \mid q_s$. Since q_s is prime, we get $p_r = q_s$. Now we can cancel $p_r = q_s$ on both sides and get

$$p_1 p_2 \dots p_{r-1} = q_1 q_2 \dots q_{s-1}.$$

By induction we can assume that $r - 1 = s - 1$ (that is, $r = s$) and, after some reordering, $p_i = q_i$ for all $i = 1, \dots, r-1$, and the statement follows. □

Corollary 7.4. *There are infinitely many prime numbers.*

Proof. Assume that there is only a finite number of prime numbers, say $p_1, \dots, p_r$ is a complete list of all prime numbers. Consider the natural number

$$n = p_1 p_2 \dots p_r + 1 > 1.$$

By the preceding theorem there is a prime number p such that $p \mid n$. There must be some i such that $p = p_i$. But $n \equiv 1 \bmod p_i$, a contradiction. □

Remark 7.5. There is the famous *Prime Number Theorem.* Denote by $\pi(x)$ the number of all prime numbers p such that $1 \leq p \leq x$. For example, the prime numbers smaller or equal than 100 are the 25 primes

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97,$$

so $\pi(100) = 25$. Similarly we have $\pi(1000) = 168$, $\pi(10000) = 1229$. The prime number theorem states that

$$\pi(x) \sim \frac{x}{\ln x}.$$

This means that the limit of the ratio $\pi(x)/(x/\ln x)$ is 1 as $x \to \infty$.

For the RSA algorithm large prime numbers with more then 100 digits are used. We can estimate the number of prime numbers with, for example, 100 digits: This number is

$$\pi(10^{100}) - \pi(10^{99}) \sim \frac{10^{100}}{\ln 10^{100}} - \frac{10^{99}}{\ln 10^{99}} \approx 3.9 \times 10^{97},$$

so there are many primes with 100 digits. App. each 230th[1] number (that is, each 115th odd number) with 100 digits is a prime number.

Remark 7.6. Let $\mathbb{P}$ be the set of all prime numbers $2, 3, 5, 7, 11, \dots$. Theorem 7.3 can be restated as follows: Any integer x with $x \neq 0$ has a unique expression

$$x = \pm \prod_{p\in\mathbb{P}} p^{\alpha_p(x)},$$

where all exponents $\alpha_p(x) \geq 0$, and are > 0 only for a finite number of $p \in \mathbb{P}$. For example,

$$-43659 = (-1) \cdot 2^0 \cdot 3^4 \cdot 5^0 \cdot 7^2 \cdot 11^1 \cdot 13^0 \cdots = -3^4 7^2 11.$$

It is then obvious, that the gcd of two non-zero integers

$$x = \pm \prod_{p\in\mathbb{P}} p^{\alpha_p(x)},$$

and

$$y = \pm \prod_{p\in\mathbb{P}} p^{\alpha_p(y)},$$

can be written in the form

$$\gcd(x, y) = \prod_{p\in\mathbb{P}} p^{\min(\alpha_p(x),\alpha_p(y))}.$$

If, for example, $x = 43659 = 3^4 7^2 11$ and $y = 61740 = 2^2 3^2 5\, 7^3$, then $\gcd(x, y) = 3^2 7^2 = 441$. But for large numbers x, y this formula is impractical for computing the gcd since factorization of integers is computationally hard. A much more efficient way to calculate the gcd is Euclid's algorithm.

Remark 7.7. With the same arguments we see:

(1) Two positive integers x and y are coprime (i.e. $\gcd(x, y) = 1$) if and only if for all prime numbers p it is true that p does not divide both x and y at the same time.

(2) Let p be prime and x any integer. Then $\gcd(x, p) = 1$ if and only if $p \nmid x$.

[1] Indeed: $10^{100} - 10^{99} = (10 - 1) \cdot 10^{99} = 9 \cdot 10^{99}$. $\frac{9\cdot 10^{99}}{3.9\cdot 10^{97}} \approx 230$.

8. Fermat's little theorem

Theorem 8.1 (Fermat's Little Theorem)**.** *Let p be prime and a be an integer, coprime to p. Then*

$$a^{p-1} \equiv 1 \bmod p.$$

Proof. Let

$$S = \{1,\, 2,\, 3, \dots,\, p-1\}.$$

Consider the map $\psi : S \to S$, $x \mapsto ax \bmod p$. In fact, $ax \bmod p \in S$, that is, $ax \bmod p \neq 0$: otherwise, since $\gcd(a,p) = 1$ we can cancel a and would get $x \bmod p = 0$, which is not true for $x \in S$.

Now, by the same reason the elements

$$\psi(1),\, \psi(2),\, \dots, \psi(p-1)$$

are pairwise different (if $\psi(x) = \psi(y)$, that is, $ax \bmod p = ay \bmod p$, then dividing by a gives $x = y$). In other words, these elements are *all* $p-1$ elements in S. In particular, multiplying all these elements gives the same result, since the order does not matter:

$$\begin{aligned} 1 \cdot 2 \cdot \dots \cdot (p-1) &= \psi(1) \cdot \psi(2) \cdot \dots \cdot \psi(p-1) \\ &\equiv (a \cdot 1) \cdot (a \cdot 2) \cdot \dots \cdot (a \cdot (p-1)) \\ &= a^{p-1} \cdot (1 \cdot 2 \cdot \dots \cdot (p-1)) \bmod p. \end{aligned}$$

Since for all $j \in S$ we have $\gcd(j,p) = 1$, we can divide both sides, step by step, first by 2, then by 3, and so on, finally by $p-1$, and get $1 \equiv a^{p-1} \bmod p$. □

Example 8.2. Compute $2^{43210} \bmod 101$.

Solution. 101 is prime, coprime to 2. By the preceding theorem we get $2^{100} \equiv 1 \bmod 101$. Therefore

$$2^{43210} = (2^{100})^{432} 2^{10} \equiv 1^{423} 2^{10} = 1024 \equiv 14 \bmod 101.$$

9. The Euler function

Definition 9.1. For any positive integer n let $\varphi(n)$ be the number of integers x which are coprime to n and such that $1 \leq x \leq n$. The function φ is called the *Euler function*, or *Euler's phi-function.*

Example 9.2. The numbers x with $1 \leq x \leq 12$ and which are coprime to 12 are 1, 5, 7, 11, so $\varphi(12) = 4$. We have $\varphi(6) = 4$ and $\varphi(2) = 1$. In particular $\varphi(2 \cdot 6) \neq \varphi(2) \cdot \varphi(6)$.

Proposition 9.3. (1) *If p is prime, then $\varphi(p) = p - 1$.*
(2) *If p is prime and $r \geq 1$, then $\varphi(p^r) = p^r - p^{r-1} = p^{r-1}(p-1)$.*
(3) *If m and n are coprime, then $\varphi(mn) = \varphi(m)\varphi(n)$.*

Proof. Obviously, (1) is a special case of (2). So we proof (2): Of the numbers $1, 2, \dots, p^r$ the only numbers which are *not* coprime to p^r are those divisible by p, so the numbers $p, 2p, 3p, \dots, p^r = p^{r-1} \cdot p$, and these are p^{r-1} many. Consequently, the remaining $p^r - p^{r-1} = p^{r-1}(p-1)$ numbers are coprime to p^r, hence $\varphi(p^r) = p^{r-1}(p-1)$.

(3) Let m and n be coprime. $\varphi(mn)$ is the number of those elements $x \in \mathbb{Z}_{mn}$, which admit a modular inverse modulo mn, by Corollary 4.2. Consider the sets $\mathbb{Z}_{mn}$ and $\mathbb{Z}_m \times \mathbb{Z}_n$. Both have mn elements. The map $\mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$, $x \mapsto (x \bmod m, x \bmod n)$ is injective by the uniqueness part of the Chinese remainder theorem, hence it is also bijective. Clearly, if x is invertible modulo mn, then it is invertible modulo m *and* modulo n. Conversely, if x is invertible modulo m and modulo n, then there are modular inverses a and b, modulo m and modulo n, respectively. The pair (a, b) of modular inverses is in the image of the above bijective map, so $(a, b) = (c \bmod m, c \bmod n)$ for a suitable $c \in \mathbb{Z}_{mn}$. Then c is a modular inverse of x, both modulo m and n. Applying 6.2 c is also an inverse of x modulo mn. We conclude the following: In $\mathbb{Z}_{mn}$ there are invertible elements modulo mn as many as pairs $(x, y) \in \mathbb{Z}_m \times \mathbb{Z}_n$, where x is invertible modulo m and y is invertible modulo n. This gives $\varphi(mn) = \varphi(m)\varphi(n)$. □

By applying this proposition, if we know a prime factorization of x we can compute $\varphi(x)$ easily:

Corollary 9.4. *Let $x = p_1^{n_1} p_2^{n_2} \dots p_r^{n_r}$ where $p_1, p_2, \dots, p_r$ are pairwise different primes, and $r_i \geq 1$. Then*

$$\varphi(x) = \prod_{i=1}^{r} \big(p_i^{n_i - 1}(p_i - 1)\big).$$

Example 9.5. We have $540 = 2^2 3^3 5$. We get

$$\varphi(540) = 2^1 \cdot (2-1) \cdot 3^2 \cdot (3-1) \cdot 5^0 \cdot (5-1) = 144.$$

Corollary 9.6. *Let p and q be two different prime numbers. Then $\varphi(pq) = (p-1) \cdot (q-1)$.*

Theorem 9.7 (Euler's Theorem)**.** *Assume that* $\gcd(a, n) = 1$. *Then*

$$a^{\varphi(n)} \equiv 1 \bmod n.$$

Note, that in the special case, where $n = p$ is a prime number, this is just Fermat's little theorem, since $\varphi(p) = p - 1$.

Proof. The proof is almost identical with the proof of Fermat's little theorem. Here the set S consists of all integers x with $1 \leq x \leq n$ such that $\gcd(x, n) = 1$, and define $\psi : S \to S$ by $\psi(x) = ax \bmod n$. (Note that in case $n = p$ is prime everything is defined in the same way as in the proof of Fermat's little theorem.) If $x \in S$, then also $\psi(x) = ax \bmod n \in S$: If not, then $\gcd(ax, n) > 1$, and there would be a common prime divisor of ax and n. The p would divide one of the factors a or x, but both is impossible, since $\gcd(a, n) = 1$ and also $\gcd(x, n) = 1$.

If now x, $y \in S$ with $\psi(x) = \psi(y)$, then $ax \equiv ay \bmod n$, and since $\gcd(a, n) = 1$, we can divide by a in order to get $x \equiv y \bmod n$, thus $x = y$. In other words, the map ψ is injective, and since S is a finite set (consisting of $\varphi(n)$ elements), ψ is also bijective. We get

$$\prod_{x\in S} x = \prod_{x\in S} \psi(x) \equiv a^{\varphi(n)} \prod_{x\in S} x \bmod n.$$

For each $x \in S$ we can divide out the factor x (since $\gcd(x, n) = 1$) and finally get $1 \equiv a^{\varphi(n)} \bmod n$. □

10. Proof that RSA is correct

Proposition 10.1. *Let $n = pq$ a product of to different primes p and q. Let x be any integer. Then*

$$x \cdot x^{\varphi(n)} \equiv x \bmod n.$$

Proof. Assume first that $\gcd(x, n) = 1$. Then by Euler's theorem $x^{\varphi(n)} \equiv 1 \bmod n$, and multiplying both sides with x gives $x \cdot x^{\varphi(n)} \equiv x \bmod n$.

Now assume $\gcd(x, n) > 1$. The only possibilities are $\gcd(x, n) = p$, q or pq. In the latter case $x \equiv 0 \bmod n$, and the assertion is clear. It remains to treat the case $\gcd(x, n) = q$ (the case $\gcd(x, n) = p$ following with the same arguments). In this case $p \nmid x$, and by Fermat's little theorem $x^{p-1} \equiv 1 \bmod p$. Then $x \cdot x^{p-1} \equiv x \bmod p$, and since $q \mid x$ we also get $x \cdot x^{p-1} \equiv x \bmod pq = n$. Now, applying this $q-1$ times we get

$$x \equiv x \cdot x^{p-1} \equiv x \cdot x^{2(p-1)} \equiv x \cdot x^{3(p-1)} \equiv \cdots \equiv x \cdot x^{(q-1)(p-1)} \bmod n.$$

□

We apply this result to show the correctness of the RSA algorithm. That is, decryption cancels encryption.

Let $n = pq$, where p and q are different primes. Let e and d be given with $ed \equiv 1 \bmod \varphi(n)$. So there is an integer k such that

$$ed = 1 + k\varphi(n).$$

Let $y = x^e \bmod n$. We have to show that $y^d \equiv x \bmod n$. Indeed,

$$\begin{aligned} y^d &\equiv x^{ed} = x^{1+k\varphi(n)} \\ &= x \cdot \left(x^{\varphi(n)}\right)^k = x \cdot x^{\varphi(n)} \cdot \left(x^{\varphi(n)}\right)^{k-1} \\ &\equiv x \cdot \left(x^{\varphi(n)}\right)^{k-1} \equiv \cdots \equiv x \bmod n. \end{aligned}$$

11. Primitive roots and discrete logarithms

Example 11.1. Consider $3 \bmod 7$ and its powers:

$$3^1 \equiv 3,\ 3^2 \equiv 2,\ 3^3 \equiv 6,\ 3^4 \equiv 4,\ 3^5 \equiv 5,\ 3^6 \equiv 1 \bmod 7.$$

We obtain *all* six non-zero congruence classes mod 7. If we consider $2 \bmod 7$ instead, then we get

$$2^1 \equiv 2,\ 2^4 \equiv 4,\ 2^3 \equiv 1,\ 2^4 \equiv 2,\ 2^5 \equiv 4,\ 2^6 \equiv 1 \bmod 7.$$

Here, we do *not* obtain all non-zero congruence classes.

Definition 11.2. Let p be a prime number. Any integer x with $1 \leq x \leq p-1$ is called a *primitive root mod p* if *each* integer y with $1 \leq y \leq p-1$ is some power $y \equiv x^i \bmod p$ of x.

Proposition 11.3. *Let g be a primitive root for the prime p.*

(1) *For any integer n, we have $g^n \equiv 1 \quad \Leftrightarrow \quad p-1 \mid n$.*
(2) $g^j \equiv g^k \bmod p \quad \Leftrightarrow \quad j \equiv k \bmod p-1$.

Proof. (2) follows from part (1), since $g^j \equiv g^k \;\Leftrightarrow\; g^{j-k} \equiv 1$.

(1) Assume $p-1 \mid n$, say $n = k \cdot (p-1)$. Then by Fermat's little theorem $g^n = (g^k)^{p-1} \equiv 1 \bmod p$. For the converse, assume $g^n \equiv 1 \bmod p$. Division with remainder gives $n = (p-1)q + r$ with $0 \leq r < p-1$. We want to show that $r = 0$. Again, by Fermat's little theorem $g^0 \equiv 1 \equiv g^n \equiv g^r \bmod p$. Assume $r > 0$. Then congruence classes of the elements in the list

$$g^1,\, g^2,\, \ldots,\, g^r \equiv 1, \ldots,\, g^{p-2},\, g^{p-1} \equiv 1$$

are not distinct, and thus g cannot be a primitive root, contradiction. We get $r = 0$, that is, $p-1 \mid n$. □

Theorem 11.4. *Let p be a prime number.*

(1) *There is a primitive root g mod p.*
(2) *g^i is also a primitive root if and only if* $\gcd(i, p-1) = 1$. *Thus, there are $\varphi(p-1)$ primitive roots modulo p.*

Proof. (1) We will not prove this.

(2) Obviously g^i is a primitive root mod p if and only if the primitive root g is some power of g^i mod p. Assume $\gcd(i, p-1) = 1$. Then there are integers x and y such that $1 = ix + (p-1)y$. Then $g = g^1 = g^{ix}(g^y)^{p-1} \equiv (g^i)^x \bmod p$. Conversely, if for some (positive) integer x we have $g \equiv (g^i)^x \bmod p$, then $g^{ix-1} \equiv 1 \bmod p$, and then by the preceding proposition $p-1 \mid ix-1$, and $\gcd(i, p-1)$ follows. □

Let p be a prime number. Let α and β be non-zero integers mod p. Assume that there is an integer y such that

$$\beta = \alpha^y \bmod p.$$

Let n be the *smallest* positive integer such that $\alpha^n \equiv 1 \bmod p$. This integer n is also called the *order* of α (mod p). A division with remainder argument shows $n \mid p-1$, since $\alpha^{p-1} \equiv 1 \bmod p$. Clearly, $n = p-1$ if and only if α is a primitive root mod p.

Lemma 11.5. *Under the preceding assumptions, there is a unique integer x with $0 \leq x < n$ and $\alpha^x = \beta$.*

Proof. We have $\beta = \alpha^y \bmod p$. If $0 \leq y < n$, we are done. Otherwise, division with remainder gives $y = nq + x$, with $0 \leq x < n$. Then $\alpha^x = (\alpha^n)^q \alpha^x = \alpha^{nq+x} = \alpha^y$. If there is a second x' with $0 \leq x \leq x' < n$ and $\alpha^x \equiv \alpha^{x'}$, then $\alpha^{x'-x} \equiv 1 \bmod p$, and since n is chosen to be the minimal such exponent, we get $x = x'$. □

Definition 11.6. If x is chosen as above, we write $x = L_\alpha(\beta)$ and call it the *discrete logarithm* (mod p) of β with respect to α.

If α is a primitive root mod p, then $L_\alpha(\beta)$ is defined for every β with $1 \leq \beta \leq p-1$. If α is not a primitive root, then $L_\alpha(\beta)$ is not defined for certain β.

Proposition 11.7. *Let α be a primitive root mod p. Then, for every β_1, β_2 (non-zero mod p) we have*

$$L_\alpha(\beta_1\beta_2) \equiv L_\alpha(\beta_1) + L_\alpha(\beta_2) \bmod p - 1.$$

Proof. Let $x_1 = L_\alpha(\beta_1)$ and $x_2 = L_\alpha(\beta_2)$. This means $\alpha^{x_1} \equiv \beta_1$, $\alpha^{x_2} \equiv \beta_2 \bmod p$ and moreover $0 \leq x_1, x_2 < n$ if n is the smallest positive integer with $\alpha^n \equiv 1 \bmod p$. But since α is a primitive root, we have $n = p-1$. Now $\alpha^{x_1+x_2} = \alpha^{x_1}\alpha^{x_2} \equiv \beta_1\beta_2 \bmod p$. By dividing x_1+x_2 by $p-1$ with remainder it follows that $L_\alpha(\beta_1\beta_2) \equiv x_1+x_2 \bmod p-1$. □

References

[1] W. Trappe and L. Washington: *Introduction to Cryptography with Coding Theory*, (2nd edition). Pearson Prentice Hall, Upper Saddle River, 2006.