Number theory

Myrto Arapinis
School of Informatics
University of Edinburgh

October 9, 2014

Division

Definition

If a and b are integers with $a \neq 0$, then a divides b if there exists an integer c such that $b = ac$

Theorem

Let a, b, c be integers, where $a \neq 0$

1. *If $a|b$ and $a|c$, then $a|(b+c)$*
2. *If $a|b$, then $a|bc$*
3. *If $a|b$ and $b|c$, then $a|c$*

Division

Definition

If a and b are integers with $a \neq 0$, then a divides b if there exists an integer c such that $b = ac$

Theorem

Let a, b, c be integers, where $a \neq 0$

1. *If $a|b$ and $a|c$, then $a|(b+c)$*
2. *If $a|b$, then $a|bc$*
3. *If $a|b$ and $b|c$, then $a|c$*

Proof

1. $a|b \;\Leftrightarrow\; \exists k_b.\; b = k_b \cdot a$ and $a|c \;\Leftrightarrow\; \exists k_c.\; c = k_c \cdot a$. But then $b + c = (k_b + k_c) \cdot a$ which by definition implies that $a|(b+c)$
2. $a|b \;\Leftrightarrow\; \exists k_b.\; b = k_b \cdot a$. But then $bc = k_b \cdot a \cdot c$ which by definition implies that $a|bc$
3. $a|b \;\Leftrightarrow\; \exists k_b.\; b = k_b \cdot a$ and $b|c \;\Leftrightarrow\; \exists k_c.\; c = k_c \cdot b$. But then $c = k_c \cdot k_b \cdot a$ which by definition implies that $a|c$

Division algorithm

Theorem

If a is an integer and d a positive integer, then there are unique integers q and r, with $0 \leq r < d$, such that $a = dq + r$

Division algorithm

Theorem

If a is an integer and d a positive integer, then there are unique integers q and r, with $0 \leq r < d$, such that $a = dq + r$

<u>Proof</u> (by contradiction) Assume $\exists q_1, q_2, r_1, r_2$ such that $a = dq_1 + r_1$, $a = dq_2 + r_2$, and $(q_1, r_1) \neq (q_2, r_2)$. But then,

$$d = \frac{r_1 - r_2}{q_2 - q_1}$$

Now since $0 \leq r_1, r_2 < m$, it must be that $-d < r_1 - r_2 < d$. But since $q_1, q_2 \in \mathbb{Z}$, it necessarily is the case that

$$-d < \frac{r_1 - r_2}{q_2 - q_1} < d$$

Which contradicts our hypothesis that $d = \frac{r_1 - r_2}{q_2 - q_1}$.

Congruence relation

Definition

If a and b are integers and m is a positive integer, then a is congruent to b modulo m, denoted $a \equiv b \pmod{m}$, iff $m | (a - b)$

Example

$17 \equiv 5 \pmod{6}$ because 6 divides $17 - 5 = 12$

$24 \equiv 14 \pmod{6}$ because $24 - 14 = 10$ is not divisible by 6

A theorem on congruences

Definition

Let m be a positive integer. The integers a and b are congruent modulo m iff there is an integer k such that $a = b + km$

A theorem on congruences

Definition

Let m be a positive integer. The integers a and b are congruent modulo m iff there is an integer k such that $a = b + km$

Proof

($\Leftarrow$) If $a \equiv b \pmod{m}$, then by the definition of congruence $m|(a-b)$. Hence, there is an integer k such that $a - b = km$ and equivalently $a = b + km$

($\Rightarrow$) If there is an integer k such that $a = b + km$, then $km = a - b$. Hence, $m|(a-b)$ and $a \equiv b \pmod{m}$

Congruences of sums, differences, and products

Theorem

Let m be a positive integer. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a + c \equiv b + d \pmod{m}$, $a - c \equiv b - d \pmod{m}$, and $ac \equiv bd \pmod{m}$

Congruences of sums, differences, and products

Theorem

Let m be a positive integer. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a + c \equiv b + d \pmod{m}$, $a - c \equiv b - d \pmod{m}$, and $ac \equiv bd \pmod{m}$

Proof

Since $a \equiv b$ (mod m) and $c \equiv d \pmod{m}$, by the Theorem above there are integers s and t with $b = a + sm$ and $d = c + tm$. Therefore, $b + d = (a + sm) + (c + tm) = (a + c) + m(s + t)$, and $bd = (a + sm)(c + tm) = ac + m(at + cs + stm)$. Hence, $a + c \equiv b + d \pmod{m}$ and $ac \equiv bd \pmod{m}$

Corollary

Let m be a positive integer and let a and b be integers. Then

- $(a + b) \text{ mod } m = ((a \text{ mod } m) + (b \text{ mod } m)) \text{ mod } m$
- $ab \text{ mod } m = ((a \text{ mod } m)(b \text{ mod } m)) \text{ mod } m$

Arithmetic modulo m

- Let $\mathbb{Z}_m = \{0, 1, \cdots, m-1\}$
- Theoperation $+_m$ is defined as $a +_m b = (a + b) \bmod m$. This is addition modulo m
- Theoperation $\cdot_m$ is defined as $a \cdot_m b = (a \cdot b) \bmod m$. This is multiplication modulo m
- Using these operations is said to be doing arithmetic modulo m

Example Find $7 +_{11} 9$ and $7 \cdot_{11} 9$
Solution Using the definitions above:
$7 +_{11} 9 = (7 + 9) \bmod 11 = 16 \bmod 11 = 5$ and
$7 \cdot_{11} 9 = (7 \cdot 9) \bmod 11 = 63 \bmod 11 = 8$

Arithmetic modulo m

The operations $+_m$ and $\cdot_m$ satisfy many of the same properties as ordinary addition and multiplication

Closure If $a, b \in \mathbb{Z}_m$, then $a +_m b$ and $a \cdot_m b$ belong to $\mathbb{Z}_m$

Associativity If $a, b, c \in \mathbb{Z}_m$, then $(a +_m b) +_m c = a +_m (b +_m c)$ and $(a \cdot_m b) \cdot_m c = a \cdot_m (b \cdot_m c)$

Commutativity If $a, b \in \mathbb{Z}_m$, then $a +_m b = b +_m a$ and $a \cdot_m b = b \cdot_m a$

Identity elements The elements 0 and 1 are identity elements for addition and multiplication modulo m, respectively. If $a \in \mathbb{Z}_m$ then $a +_m 0 = a$ and $a \cdot_m 1 = a$

Additive inverses If $0 \neq a \in \mathbb{Z}_m$, then $m - a$ is the additive inverse of a modulo m. Moreover, 0 is its own additive inverse $a +_m (m - a) = 0$ and $0 +_m 0 = 0$

Distributivity If $a, b, c \in \mathbb{Z}_m$, then $a \cdot_m (b +_m c) = (a \cdot_m b) +_m (a \cdot_m c)$ and $(a +_m b) \cdot_m c = (a \cdot_m c) +_m (b \cdot_m c)$

Multiplicative inverses

Addition and multiplication mod m is easy. What about division?

Multiplicative inverses

Addition and multiplication mod m is easy. What about division?

- Over the reals, dividing by a number x is the same as multiplying by $y = 1/x$

Multiplicative inverses

Addition and multiplication mod m is easy. What about division?

- Over the reals, dividing by a number x is the same as multiplying by $y = 1/x$
- Similarly when we wish to divide by x mod m, we wish to find y mod m such thatx $x \cdot y \equiv 1 \pmod{m}$

Multiplicative inverses

Addition and multiplication mod m is easy. What about division?

- Over the reals, dividing by a number x is the same as multiplying by $y = 1/x$
- Similarly when we wish to divide by x mod m, we wish to find y mod m such thatx $x \cdot y \equiv 1 \pmod{m}$

Example Let $x = 8$ and $m = 15$. Then $2x = 16 \equiv 1 \pmod{15}$, so 2 is a multiplicative inverse of 8 $\pmod{15}$

Multiplicative inverses

Addition and multiplication mod m is easy. What about division?

- Over the reals, dividing by a number x is the same as multiplying by $y = 1/x$
- Similarly when we wish to divide by x mod m, we wish to find y mod m such thatx $x \cdot y \equiv 1 \pmod{m}$

<u>Example</u> Let $x = 8$ and $m = 15$. Then $2x = 16 \equiv 1 \pmod{15}$, so 2 is a multiplicative inverse of 8 (mod 15)

<u>Example</u> Let $x = 12$ and $m = 15$. Then the sequence $\{ax \pmod{m} \mid a = 0, 1, 2, ...\}$ is periodic, and takes on the values $\{0, 12, 9, 6, 3\}$. Thus 12 has no multiplicative inverse mod 15

Multiplicative inverses

Addition and multiplication mod m is easy. What about division?

- Over the reals, dividing by a number x is the same as multiplying by $y = 1/x$
- Similarly when we wish to divide by x mod m, we wish to find y mod m such thatx $x \cdot y \equiv 1 \pmod{m}$

Example Let $x = 8$ and $m = 15$. Then $2x = 16 \equiv 1 \pmod{15}$, so 2 is a multiplicative inverse of 8 (mod 15)

Example Let $x = 12$ and $m = 15$. Then the sequence $\{ax \pmod{m} \mid a = 0, 1, 2, \ldots\}$ is periodic, and takes on the values $\{0, 12, 9, 6, 3\}$. Thus 12 has no multiplicative inverse mod 15

Not all integers have an inverse mod m

Primes

Definition

A positive integer $p > 1$ is called prime iff the only positive factors of p are 1 and p. Otherwise it is called composite

Theorem (Fundamental Theorem of Arithmetic)

Every positive integer greater than 1 can be written uniquely as a prime or as the product of its prime factors, written in order of nondecreasing size.

Proof by induction (see slides on induction)

Example $765 = 3 \cdot 3 \cdot 5 \cdot 17 = 3^2 \cdot 5 \cdot 17$

There are infinitely many primes - Euclid (325-265 BCE)

Lemma Every natural number greater than one is either prime or it has a prime divisor

There are infinitely many primes - Euclid (325-265 BCE)

Lemma Every natural number greater than one is either prime or it has a prime divisor

Proof Suppose towards a contradiction that there are only finitely many primes $p_1, p_2, p_3, \ldots, p_k$. Consider the number $q = p_1 p_2 p_3 \ldots p_k + 1$, the product of all the primes plus one. By hypothesis q cannot be prime because it is strictly larger than all the primes. Thus, by the lemma, it has a prime divisor, p. Because $p_1, p_2, p_3, \ldots, p_k$ are all the primes, p must be equal to one of them, so p is a divisor of their product. So we have that p divides $p_1 p_2 p_3 \ldots p_k$, and p divides q, but that means p divides their difference, which is 1. Therefore $p \leq 1$. Contradiction. Therefore there are infinitely many primes. $\square$

The Sieve of Eratosthenes (276-194 BCE)

How to find all primes between 2 and n?

The Sieve of Eratosthenes (276-194 BCE)

How to find all primes between 2 and n?

A very inefficient method of determining if a number n is prime

Try every integer $i \leq \sqrt{n}$ and see if n is divisible by i:

1. Write the numbers $2, \ldots, n$ into a list. Let $i := 2$
2. Remove all strict multiples of i from the list
3. Let k be the smallest number present in the list s.t. $k > i$. Then let $i := k$
4. If $i > \sqrt{n}$ then stop else go to step 2

Testing if a number is prime can be done efficiently in polynomial time [Agrawal-Kayal-Saxena 2002], i.e., polynomial in the number of bits used to describe the input number. Efficient randomized tests had been available previously.

Greatest common divisor

Definition

Let $a, b \in \mathbb{Z} - \{0\}$. The largest integer d such that $d|a$ and also $d|b$ is called the greatest common divisor of a and b. It is denoted by $\gcd(a, b)$

Example $\gcd(24, 36) = 12$

Greatest common divisor

Definition

Let $a, b \in \mathbb{Z} - \{0\}$. The largest integer d such that $d|a$ and also $d|b$ is called the greatest common divisor of a and b. It is denoted by $\gcd(a, b)$

Example $\gcd(24, 36) = 12$

Definition

The integers a and b are relatively prime (coprime) iff $\gcd(a, b) = 1$

Example 17 and 22 (Note that 22 is not a prime)

Gcd by Prime Factorizations

Suppose that the prime factorizations of a and b are:

$$a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n} \qquad\qquad b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n}$$

where each exponent is a nonnegative integer (possibly zero). Then

$$\gcd(a, b) = p_1^{\min(a_1, b_1)} p_2^{\min(a_2, b_2)} \cdots p_n^{\min(a_n, b_n)}$$

This number clearly divides a and b. No larger number can divide both a and b. Proof by contradiction and the prime factorization of a postulated larger divisor.

Factorization is a very inefficient method to compute gcd. The Euclidian algorithm is much better.

Euclidian algorithm

Euclidian algorithm

```
algorithm gcd(x,y)
    if y = 0
    then return(x)
    else return(gcd(y,x mod y))
```

Thed Euclidian algorithm relies on the fact that
$\forall x, y \in \mathbb{Z}.\ x > y \rightarrow \mathrm{gcd}(x, y) = \mathrm{gcd}(y, x \bmod y)$

Euclidian algorithm (proof of correctness)

Lemma

Let $a = bq + r$,where a, b, q, and r are integers. Then $\gcd(a, b) = \gcd(b, r)$

Euclidian algorithm (proof of correctness)

Lemma

Let $a = bq + r$,where a, b, q, and r are integers. Then $\gcd(a, b) = \gcd(b, r)$

Proof

($\Rightarrow$) Suppose that d divides both a and b. Then d also divides $a - bq = r$. Hence, any common divisor of a and b must also be a common divisor of b and r

($\Leftarrow$) Suppose that d divides both b and r. Then d also divides $bq + r = a$. Hence, any common divisor of b and r must also be a common divisor of a and b.

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

Multiplicative inverses

Theorem

Let m, x be positive integers. $gcd(m, x) = 1$ iff x has a multiplicative inverse modulo m (and it is unique (modulo m)).

Multiplicative inverses

Theorem

Let m, x be positive integers. $gcd(m, x) = 1$ iff x has a multiplicative inverse modulo m (and it is unique (modulo m)).

Proof ($\Rightarrow$) Consider the sequence of m numbers $0, x, 2x, ...(m-1)x$. We first show that these are all distinct modulo m.
To verify the above claim, suppose that $ax \bmod m = bx \bmod m$) for two distinct values a, b in the range $0 \leq a, b \leq m-1$. Then we would have $(a-b)x \equiv 0 (\bmod\ m)$, or equivalently, $(a-b)x = km$ for some integer k. But since x and m are relatively prime, it follows that $a-b$ must be an integer multiple of m. This is not possible since a,b are distinct non-negative integers less than m.
Now, since there are only m distinct values modulo m, it must then be the case that $ax \equiv 1 (\bmod\ m)$ for exactly one a (modulo m). This a is the unique multiplicative inverse.

Gcd as a linear combination

Theorem (Bézout's theorem)

If x and y are positive integers, then there exist integers a and b such that $gcd(x, y) = ax + by$ (Proof in exercises of Section 5.2)

Example $2 = \gcd(6, 14) = (-2) \cdot 6 + 1 \cdot 14$

Extended Euclidian algorithm

The Bézout coefficients can be computed as follows:

```
algorithm extended-gcd(x,y)
    if y = 0
    then return(x, 1, 0)
    else
     (d, a, b) := extended-gcd(y, x mod y)
     return((d, b, a - (x div y) * b))
```

The multiplicative group $\mathbb{Z}_m^*$

Definition

Let $\mathbb{Z}_m^* = \{x \mid 1 \leq x < m \text{ and } \gcd(x, m) = 1\}$. Together with multiplication modulo m, this is called the multiplicative group modulo m. It is closed, associative, has a neutral element (namely 1) and every element has an inverse.

Fermat's little theorem

Theorem

If p is prime and $p \not| a$, then $a^{p-1} \equiv 1 \ (mod\ p)$. Furthermore, for every integer a we have $a^p \equiv a \ (mod\ p)$

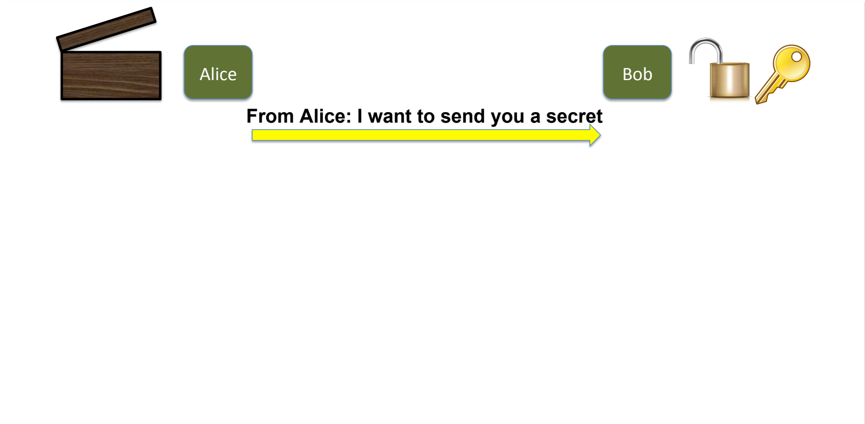
Fermat's little theorem is useful in computing the remainders modulo p of large powers of integers

<u>Example</u> Find 7^{222} mod 11

By Fermat's little theorem, we know that $7^{10} \equiv 1 \pmod{11}$, and so $(7^{10})^k \equiv 1 \pmod{11}$ for every positive integer k. Therefore, $7^{222} = 7^{22=\cdot 10+2} = (7^{10})^{22} \cdot 7^2 \equiv 122 \cdot 49 \equiv 5 \pmod{11}$. Hence, 7^{222} mod $11 = 5$

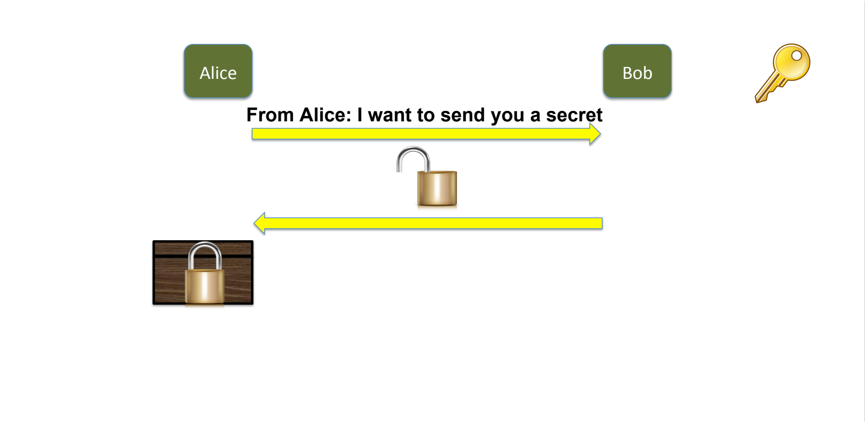
Public-key encryption in pictures

Public-key encryption in pictures

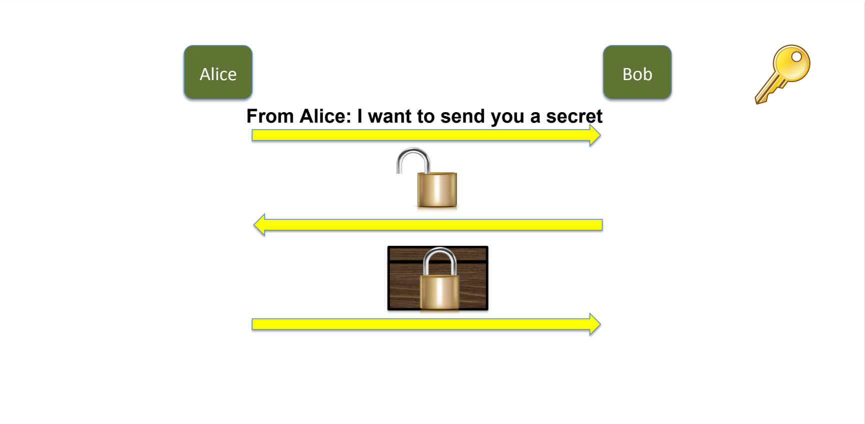


Public-key encryption in pictures

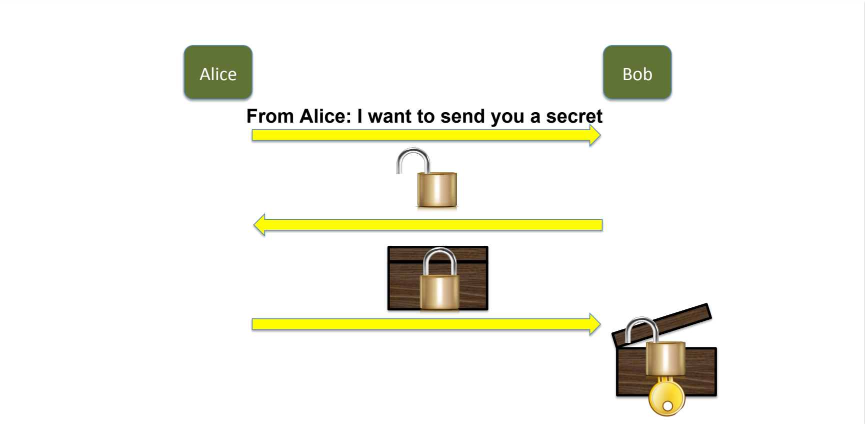
Public-key encryption in pictures



Public-key encryption in pictures



Public-key encryption in pictures



RSA: key generation

- Choose two distinct prime numbers p and q. Prime integers can be efficiently found using a primality test
- Let $n = pq$ and $k = (p-1)(q-1)$. (In particular, $k = |\mathbb{Z}_n|$)
- Choose an integer e such that $1 < e < k$ and $\gcd(e, k) = 1$; i.e. e and k are coprime
- (n, e) is released as the public key
- Let d be the multiplicative inverse of e modulo k, i.e. $de \equiv 1 \pmod{k}$. (Computed using the extendedE uclidean algorithm)
- (n, d) is the private key and kept secret

RSA: encryption and decryption

Alice transmits her public key (n, e) to Bob and keeps the private key secret

Encryption If Bob wishes to send message M to Alice.

1. He turns M into an integer m, such that $0 \leq m < n$ by using an agreed-upon reversible protocol known as a padding scheme
2. He computes the ciphertext c corresponding to $c = m^e \bmod n$. This can be done quickly using the method of exponentiation by squaring.
3. Bob transmits c to Alice.

Decryption Alice can recover m from c by

1. Using her private key exponent d via computing $m = c^d \bmod n$
2. Given m, she can recover the original message M by reversing the padding scheme

RSA: correctness of decryption

Given that $c = m^e$ mod n, is $m = c^d \bmod n$?

$$c^d = (m^e)^d \equiv m^{ed} \pmod{n}$$

By construction, d and e are each others multiplicative inverses modulo k, i.e. $ed \equiv 1 \pmod{k}$. Also $k = (p-1)(q-1)$. Thus $ed - 1 = h(p-1)(q-1)$ for some integer h. We consider $m^{ed} \bmod p$

If $p \not| m$ then

$m^{ed} = m^{h(p-1)(q-1)}m = (m^{p-1})^{h(q-1)}m \equiv 1^{h(q-1)}m \equiv m \pmod{p}$

(by Fermat's little theorem)

Otherwise $m^{ed} \equiv 0 \equiv m \pmod{p}$

Symmetrically, $m^{ed} \equiv m \pmod{q}$

Since p, q are distinct primes, we have $m^{ed} \equiv m \pmod{pq}$. Since $n = pq$, we have $c^d m^{ed} \equiv m \pmod{n}$