Number Theory, Lecture 12

Assorted topics

Jan Snellman[1]

[1]Matematiska Institutionen
Linköpings Universitet

Summary

Summary

Summary

1. RSA
2. Integer part function
3. Decimal fractions

RSA public key cryptosystem

- Used to transfer short messages, e.g. keys for symmetric ciphers
- Public key: A,B both have a private, secret key and a public, open key
- A can send an encoded message to B, without prior arrangement
- The eavesdropper Eve can not decode the message, even when in possession of the encrypted message and the public part of A's and B's keys
- B can make use of her secret, private key to decrypt the message
- If Eve wants to brute-force decrypt the message, must factor a large integer, computationally infeasible

- B has secret: two large primes p, q.
- B makes public: $n = pq$, e positive integer with $\gcd(e, \phi(n)) = 1$.
- A sends message to B: breaks up into "letters" or "blocks", integers $0 \leq P < n$
- Encodes each "block" and sends it: $E(P) = C \equiv P^e \mod n$, $0 \leq C < n$.
- B receives C, and decrypt by $D(C) = C^d$ where d multiplicative inverse of e modulo $\phi(n)$, easily computed by B since B knows factorization $n = pq$, thus $\phi(pq) = \phi(p)\phi(q) = (p-1)(q-1)$. Extended Euclidean algorithm finds d, k such that $ed = k\phi(n) + 1$, throw away k.

- We see that

$$C^d \equiv (P^e)^d \equiv P^{ed} \equiv P^{k\phi(n)+1} \equiv P^{\phi(n)^k} P \equiv P \mod n$$

  assuming $\gcd(P, n) = 1$
- In most cases, $\gcd(P, n) = 1$, probability $1 - 1/p - 1/q + 1/pq$
- If $\gcd(P, pq) > 1$ then either $p|P$ or $p \not| P$.
- If $p \not| P$, then $D(C) = P^{(p-1)(q-1)k} P \equiv P \mod p$, by Fermat.
- If $p|P$, then $P \equiv 0 \mod p$, but also $D(C) = P^e \equiv 0 \mod p$
- Similarly, $D(C) \equiv P \mod q$.
- By CRT, $D(C) \equiv P \mod pq$.
- Note that if $s = \gcd(P, n) > 1$, and r is a prime factor of s, then since $r|pq$ we have that $r = p$ or $r = q$, so Eve can factor n, and decrypt the message!

Definition

A positive integer n is perfect iff $\sigma(n) = 2n$, where $\sigma(n) = \sum_{k|n} 1$.

Thus n is perfect iff

$$n = \sum_{\substack{k|n \\ 1 \leq k < n}} 1.$$

Example

$6 = 1 + 2 + 3$ is perfect, $7 \neq 1$ is not.

Theorem

n is even and perfect iff $n = 2^{m-1}(2^m - 1)$ with $m \geq 2$, $2^m - 1$ prime.

Proof

- σ multiplicative, $\sigma(p^a) = \frac{p^{a+1}-1}{p-1}$ on prime powers
- Assume n of above form.
- 2^m even, $2^m - 1$ odd, $\gcd(2^{m-1}, 2^m - 1) = 1$
- $\sigma(n) = \sigma(2^{m-1})\sigma(2^m - 1) = (2^m - 1)2^m = 2n$, so n is perfect.
- Now assume $n = 2^s t$ perfect, $s \geq 1$, t odd.
- $\sigma(n) = \sigma(2^s)\sigma(t) = (2^{s+1} - 1)\sigma(t) = 2n = 2^{s+1}t$ so $(2^{s+1} - 1)\sigma(t) = 2^{s+1}t$.
- $2^{s+1} | RHS \implies 2^{s+1} | LHS \implies 2^{s+1} | \sigma(t)$

Proof (cont)

- $\sigma(t) = 2^{s+1}q$
- $(2^{s+1}-1)2^{s+1}q = 2^{s+1}t$
- $(2^{s+1}-1)q = t$
- $q|t$, $t > q$.
- $(2^{s+1}-1)q + q = 2^{s+1}q = t + q$, so $\sigma(t) = t + q$
- If $q > 1$ then $1, q, t$ all divide t, so $sigma(t) \geq 1 + q + t$, a contradiction. Hence $q = 1$.
- So $t = 2^{s+1} - 1$.
- Furthermore, $\sigma(t) = t + 1$, so t prime.

Theorem

$2^m - 1$ *is only prime when* m *is prime.*

Proof.

If $m = ab$ then

$$2^m - 1 = (2^a - 1)(2^{a(b-1)} + 2^{a(b-2)} + \cdots + 2^a + 1$$

□

Definition

$M_n = 2^m - 1$ m'th Mersenne number, M_p Mersenne prime (if prime).

Example

$M_7 = 2^7 - 1$ prime, $M_{11} = 2^{11} - 1 = 23 * 89$

Theorem

p odd prime. Then any divisor of $M_p = 2^p - 1$ is of the form $2kp + 1$.

Proof.

Check Rosen! □

- There are more efficient primality tests for M_p, see Rosen
- Largest known M_p: $p \approx 10^8$, $M_p \approx 10^{10^8}$

Definition

For $x \in \mathbb{R}$, $\lceil x \rceil$ is the largest integer $\leq x$.

Example

$\lfloor 7/3 \rfloor = 2$.

Theorem

$x \in \mathbb{R}$, $n \in \mathbb{Z}$.

- $x - 1 < \lfloor x \rfloor \leq x < \lfloor x \rfloor + 1$
- $\lfloor x + n \rfloor = \lfloor x \rfloor + n$
- $\lfloor \frac{\lfloor x \rfloor}{n} \rfloor = \lfloor \frac{x}{n} \rfloor$
- $\lfloor x \rfloor + \lfloor -x \rfloor = \begin{cases} 0 & x \in \mathbb{Z} \\ -1 & x \notin \mathbb{Z} \end{cases}$

Theorem

$m, n \in \mathbb{Z},\ m, n > 0$. *Then*

$$\lfloor m/n \rfloor - \lfloor (m-1)/n \rfloor = \begin{cases} 1 & n|m \\ 0 & n \not| m \end{cases}$$

Proof.

If $m = kn$ *then* $\lfloor m/n \rfloor = k$, *and* $\lfloor (m-1)/n \rfloor = k-1$, *so* $\lfloor m/n \rfloor - \lfloor (m-1)/n \rfloor = 1$.
If $m = kn + r$, $0 < r < n$, *then* $k = \lfloor m/n \rfloor$, *and*

$$\lfloor \frac{m-1}{n} \rfloor = \lfloor \frac{kn+r-1}{n} \rfloor = k + \lfloor \frac{r-1}{n} \rfloor = k + 0 = k$$

so $\lfloor m/n \rfloor - \lfloor (m-1)/n \rfloor = 0$. □

Theorem

n positive integer. Then

$$\lfloor \sqrt{n} \rfloor - \lfloor \sqrt{n-1} \rfloor = \begin{cases} 1 & n \text{ is a perfect square} \\ 0 & \text{otherwise} \end{cases}$$

Theorem

- $$\lfloor x \rfloor /2 = \lfloor x/2 \rfloor + \begin{cases} 0 & 2 | \lfloor x \rfloor \\ 1/2 & 2 \not| \lfloor x \rfloor \end{cases}$$
- $$\lfloor (x+1)/2 \rfloor = \begin{cases} \lfloor x \rfloor /2 & 2 | \lfloor x \rfloor \\ (\lfloor x \rfloor + 1)/2 & 2 \not| \lfloor x \rfloor \end{cases}$$

Theorem

Let m, n be positive integers, with $\gcd(m,n) = d$. *Then*

$$\sum_{j=1}^{n-1} \lfloor jm/n \rfloor = \frac{1}{2}(m-1)(n-1) + \frac{1}{2}(d-1)$$

If $d = 1$ then

$$\sum_{j=1}^{n-1} \lfloor jm/n \rfloor = \sum_{j=1}^{m-1} \lfloor jn/m \rfloor = \frac{1}{2}(m-1)(n-1)$$

Definition

Let $x \in \mathbb{R}$, $0 \leq x < 1$, and let b be a positive integer. Then x can be written as

$$x = \sum_{j=1}^{\infty} c_j b^{-j},$$

and this expression is unique if we demand that there are infinitely many j s.t. $c_j \neq b-1$.
We write

$$x = 0.c_1 c_2 c_3 \ldots$$

after specifying the base b.

Example

In base 2, we write

$$\frac{1}{2} = 0.10000\ldots$$

rather than

$$\frac{1}{2} = 0.0111111\cdots = 1/4 + 1/8 + 1/16 + \ldots$$

Lemma

Let $x_n = b^n \sum_{j=n+1}^{\infty} c_j b^{-j}$ *so that*

$$x = \sum_{j=1}^{\infty} c_j b^{-j} = c_1/b + \ldots c_n/b^n + x_n/b^n$$

Then

$$\begin{aligned} c_1 &= \lfloor bx \rfloor \\ x_1 &= bx - c_1 \\ c_k &= \lfloor bx_{k-1} \rfloor \\ x_k &= bx_k - c_k \end{aligned}$$

Example

Let $b = 2$, $x = 1/3$. Then

$$\begin{aligned} c_1 &= \lfloor 2/3 \rfloor = 0 \\ x_1 &= 2/3 - 0 = 2/3 \\ c_2 &= \lfloor 4/3 \rfloor = 1 \\ x_2 &= 4/3 - 1 = 1/3 \\ c_3 &= \lfloor 2/3 \rfloor = 0 \\ x_3 &= 2/3 - 0 = 2/3 \end{aligned}$$

Since $x_3 = x_1$, the binary expansion repeats, with $c_2 = c_4 = c_6 = c_8 = \cdots = 1$, $c_1 = c_3 = c_5 = c_7 = \cdots = 0$, so

$$x = 1/3 = 0.0101010101\ldots$$

in base 2.

Definition

The base-b expansion of x terminates if $c_n = 0$ for all sufficiently large n. It is periodic with pre-period N and (least) period d if

$$c_{j+d} = c_j \text{ for all } j > N$$

and d is the smallest positive integer with this property.

Example

The binary expansion $1/3 = 0.01010101\ldots$ is periodic with period 2, and pre-period 0. $5/6 = 1/2 + 1/3 = 0.11010101\ldots$ is periodic with period 2, and pre-period 1.

Lemma

If x has a terminating or periodic expansion, then x is rational.

Proof.

First assertion: obvious.

Second assertion: assume

$$x = 0.a_1 a_2 \dots a_N \overline{c_1 \dots c_d}$$

Let $y = x - \sum_{j=1}^{N} a_j b^{-j} = 0.\overline{c_1 \dots c_d}$; clearly y is rational iff x is. But

$$\begin{aligned} y &= (c_1 b^{-1} + \dots c_d b^{-d}) + (c_1 b^{-d-1} + \dots c_d b^{-2d}) + \dots \\ &= b^{-1}(c_1 + \dots c_d b^{-d+1})(1 + b^d + b^{2d} \dots) \\ &= \frac{b^{-1}(c_1 + \dots c_d b^{-d+1})}{1 - b^d} \end{aligned}$$

which is rational. □

Example

Let x have binary expansion $0.111010010100101001\ldots$ Then $y = 0.1010010100\cdots = x - 0.11 = x - 3/4$, and furthermore $2^6 y = 10100.10100101\cdots = (10100)_2 + y = 32 + 8 + y = 40 + y$, so $y = 40/(2^6 - 1)$, $x = y + 3/4$.

Lemma

If x is rational, then it has a terminating or periodic expansion.

Proof.

Let $x = r/s$. Recall that $c_k = \lfloor bx_{k-1} \rfloor$, $x_k = bx_{k-1} - c_k$, and that $0 \leq x_k < 1$. By induction, one can prove that $x_k \in \frac{1}{s}\mathbb{Z}$, thus x_k can attain at most $s+1$ different values; inevitably, there will be a collision. □

Theorem

Let $b > 1$ be an integer, $x = r/s$ with $\gcd(r,s) = 1$, $0 < r < s$, and write $s = TU$ with T containing the prime factors of s that also occur in b, and U the rest.
Then

1. *the period length of the base-b expansion of x is $\mathrm{ord}_U(b)$, the order of $[b]_U \in \mathbb{Z}_U^\times$.*
2. *the preperiod is N, the smallest positive integer s.t. $T | b^N$.*

In particular, x has terminating base-b expansion iff $U = 1$.
If b is prime, then $T = b^\ell = v_b(s)$, $\mathrm{ord}_U(b)$ still needs to be computed, but the preperiod simplifies to ℓ.

Example

Let $b = 2$, $x = 13/17$. Then since $17 = 2^0 * 17$, the pre-period of the binary expansion of x is zero. The period is $\mathtt{ord}_{17}(2) = 8$. Indeed,

$$13/17 = 0.11000011\,11000011\,11000011\,11000011\,11000100\ldots$$