COMP 3704 Computer Security

Christian Grothoff
christian@grothoff.org

http://grothoff.org/christian/

Definition: Divisor

Let $m \neq 0$ and $n, m \in \mathbb{Z}$, then m **divides** n if there exists a $q \in \mathbb{Z}$ such that $n = mq$.

We then also say that n is a multiple of q.

We write $d|a$ and say d divides a.

Rules

$$m|n \Leftrightarrow n\%m = 0 \quad (1)$$

$$n|0 \wedge n|n \qquad \text{for } n \neq 0 \quad (2)$$

$$m|n \Rightarrow -m|n \wedge m|-n \quad (3)$$

$$1|n \qquad \text{for all } n \quad (4)$$

$$m|n \wedge n \neq 0 \Rightarrow |m| \leq |n| \quad (5)$$

$$n|1 \Rightarrow |n| = 1 \quad (6)$$

More Rules

$$m|n \wedge n|m \Rightarrow n = m \vee n = -m \tag{7}$$

$$m|n \Leftrightarrow lm|ln \qquad \text{if } l \neq 0 \tag{8}$$

$$m|n_1 \wedge m|n_2 \Rightarrow m|(l_1n_1 + l_2n_2) \qquad \text{for all } l_1, l_2 \tag{9}$$

$$m_1|n_1 \wedge m_2|n_2 \Rightarrow m_1m_2|n_1n_2 \tag{10}$$

UNIVERSITY OF DENVER

Definition: Prime Numbers

Let $\tau(n)$ be the number of positive divisors for $n \in \mathbb{N}$.

A **prime number** p is a natural number with exactly two positive divisors ($1|p$ and $p|p$):

$$\tau(p) = 2. \tag{11}$$

Fundamental Theorem of Arithmetic

Every positive integer can be represented in exactly one way (modulo permutations) as a product of zero or more primes.

Greatest Common Divisor

$d = GCD(a, b)$ if $d \in \mathbb{N}$ is the largest number such that $d|a$ and $d|b$.

Euclidean Algorithm

```
unsigned int gcd(unsigned int a, unsigned int b)
  unsigned int g = b;
  while (a > 0) {
    g = a;
    a = b % a;
    b = g;
  }
  return g;
}
```

Definition: Coprime

Two numbers $a, b \in \mathbb{Z}$ are called **coprime**, **relatively prime** or **strangers** if $GCD(a, b) = 1$.

Multiplicative Functions

A function $f : \mathbb{Z} \longrightarrow \mathbb{C}$ is called **multiplicative** if

$$f(n_1 \cdot n_2) = f(n_1) \cdot f(n_2) \tag{12}$$

for all coprime numbers $n_1, n_2 \in \mathbb{N}$.

Product of Infinite Series

If $f : \mathbb{Z} \longrightarrow \mathbb{C}$ multiplicative and $\sum_{n=1}^{\infty} f(n)$ is absolutely convergent, then:

$$\sum_{n=1}^{\infty} f(n) = \prod_{p} \sum_{v=0}^{\infty} f(p^v). \tag{13}$$

(using fundamental theorem of arithmetic).

Riemann Zeta Function

$\zeta : \mathbb{C} \rightarrow \mathbb{C}$ is for $Re\ s > 1$ defined as:

$$\zeta(s) := \sum_{n=1}^{\infty} n^{-s} \tag{14}$$

$$= \prod_{p} \sum_{v \geq 0} p^{-sv} \tag{15}$$

$$= \prod_{p} (1 - p^{-s})^{-1}. \tag{16}$$

Proof: Using product of infinite series and summation of geometric series.

Euclid

"There are infinitely many primes."

Non-standard **Proof:**

$$\zeta(2) = \sum_{n \in \mathbb{N}} n^{-2} = \frac{1}{6}\pi^2 \notin \mathbb{Q}. \tag{17}$$

Modular Arithmetic

- $a = a + (b \cdot n) \mod n$ for $a, b \in \mathbb{Z}$, $n \in \mathbb{N}$
- $a \cdot b \equiv (a \mod n) \cdot (b \mod n) \mod n$

We call the resulting ring $\mathbb{Z}_n$.

For p prime, $\mathbb{Z}_p \equiv \mathbb{F}_p$ is a field.

Modular Exponentiation (1/2)

How to calculate $a^{14} \mod n$?

1. $a_1 \equiv a \mod n$
2. $a_2 \equiv a_1 \cdot a_1 \mod n$
3. $a_4 \equiv a_2 \cdot a_2 \mod n$
4. $a_8 \equiv a_4 \cdot a_4 \mod n$
5. $a_{12} \equiv a_8 \cdot a_4 \mod n$
6. $a_{14} \equiv a_{12} \cdot a_2 \mod n$

Modular Exponentiation (2/2)

How to calculate $a^{14} \mod n$ in parallel?

1. $a_1 \equiv a \mod n$
2. $a_2 \equiv a_1 \cdot a_1 \mod n$
3. $a_3 \equiv a_1 \cdot a_2 \mod n$ and $a_4 \equiv a_2 \cdot a_2 \mod n$
4. $a_7 \equiv a_3 \cdot a_4 \mod n$
5. $a_{14} \equiv a_7 \cdot a_7 \mod n$

Inverses $\mod n$

Given $a \in \mathbb{Z}_n$, find $x \in \mathbb{Z}_n$ such that

$$a \cdot x \equiv 1 \mod n. \tag{18}$$

We also write

$$a^{-1} \equiv x \mod n. \tag{19}$$

a^{-1} exists $\mod n$ if a and n are coprime.

Computing Inverses $\mod n$

Extended Euclidean algorithm finds x and y in

$$ax + by = GCD(a, b). \tag{20}$$

If a and b are coprime, then

$$ax + by = 1 \tag{21}$$

$$\Rightarrow ax \equiv 1 \mod b \tag{22}$$

$$\Rightarrow a^{-1} \equiv x \mod n \tag{23}$$

UNIVERSITY OF DENVER

Extended Euclidean Algorithm

```
fun extended_gcd(a, b)
    if a mod b = 0
        (0, 1, b)
    else let
        (x, y, g) = extended_gcd(b, a mod b)
    in
        (y, x - y * (a div b), g)
    end
```

Homework

Either:

- Learn about functional programming, or
- Understand Schneier's version on pages 246-248

Fermat's Little Theorem

Let p be prime. Then

$$a^p \equiv a \mod p \tag{24}$$

for any a. If $p \not| a$ then

$$a^{p-1} \equiv 1 \mod p \tag{25}$$

Euler's Totient Function

$$\begin{aligned}\phi_\alpha(n) := \#\Big\{(l_1,\ldots,l_\alpha) \in \{1,\ldots,n\}^\alpha :\\ GCD(l_1,\ldots,l_\alpha,n) = 1\Big\}\end{aligned} \tag{26}$$

In particular $\phi(n) := \phi_1(n)$ is the number of natural numbers smaller than n that are coprime to n.

Computing Euler's Totient Function

- $\phi(p) = p - 1$.
- $\phi(p^j) = p^{j-1} \cdot (p - 1)$.
- $\phi(n)$ is multiplicative.

Euler's Theorem

Let $a, m \in \mathbb{N}$ be coprime. Then

$$a^{\phi(m)} \equiv 1 \mod m. \tag{27}$$

Factoring

- Factoring is $assumed$ to be a hard problem.
- If not, a lot of cryptography breaks down.
- Complexity has not been established, but is likely not in P or NP.
- The hardest problem is factoring products of two randomly-chosen primes of about the same size, but not too close.

UNIVERSITY OF DENVER

Evidence of Complexity of Factoring

- General number field sieve for b-bit number has complexity

$$O\left(exp\left(\left(\frac{64}{9}b\right)^{\frac{1}{3}}(\log b)^{\frac{2}{3}}\right)\right). \tag{28}$$

- RSA 640 has been factored, RSA-704 is still pending.

Prime Number Generation

- Factoring is hard

$\Rightarrow$ Cannot generate primes efficiently by factoring

- Use statistical tests:
  - For a $random$ number t, non-primes pass with probability $1 - p$

$\Rightarrow$ Number passing n tests is prime with probability $1 - p^n$.

Lehmann

1. Choose a random number a less than p.
2. Calculate $t \equiv a^{(p-1)/2} \mod p$.
3. If $t \neq \pm 1 \mod p$ then p is not prime.
4. Otherwise the likelihood that p is not prime is no more than 50%.

Rabin-Miller

Calculcate m such that $p = 1 + 2^b \cdot m$ using the largest b with $2^b | p - 1$.

1. Choose a random positive number $a \neq 1$ less than p.
2. Set $j = 0$ and $z \equiv a^m \mod p$
3. If $z = 1$ or $z = p - 1$ then p maybe prime.
4. If $j > 0$ and $z = 1$, then p is not prime.
5. Set $j = j + 1$. If $j < b$ and $z \neq p - 1$ set $z \equiv z^2 \mod p$ and go back to step 4.
6. If $j = b$ and $z \neq p - 1$ then p is not prime.

Prime Number Generation

1. Choose a random n-bit number p.
2. Set the high-order and low-order bit to 1.
3. Check that p is not divisible by any small primes (3, 5, 7, 11).
4. Perform Rabin-Miller test n times. If it ever fails, goto step 1.

Naturally, step 3 is optional, but generally cheaper than Rabin-Miller.

Discrete Logarithms

Given $a, b \in \mathbb{Z}_n$, find $x \in \mathbb{Z}_n$ such that

$$a^x \equiv b \mod n. \tag{29}$$

We also write

$$\log_a b \equiv x \mod n. \tag{30}$$

Questions

?

Problem

Show that:

$$m|n_1 \wedge m|n_2 \Rightarrow m|(l_1n_1 + l_2n_2) \qquad \text{for all } l_1, l_2 \tag{31}$$

$$m_1|n_1 \wedge m_2|n_2 \Rightarrow m_1m_2|n_1n_2 \tag{32}$$

Problem

Find values for a, b and m such that there is no x with

$$\log_a b \equiv x \mod n. \tag{33}$$