

CS355: Cryptography

Lecture 8: Basic Number Theory

Divisibility

Definition

Given integers a and b , with $a \neq 0$, a divides b (denoted $a|b$) if \exists integer k , s.t. $b = ak$.

a is called a **divisor** of b , and b a **multiple** of a .

Proposition:

(1) If $a \neq 0$, then $a|0$ and $a|a$. Also, $1|b$ for every b

(2) If $a|b$ and $b|c$, then $a|c$.

(3) If $a|b$ and $a|c$, then $a|(sb + tc)$ for all integers s and t .

Divisibility (cont.)

Theorem (Division algorithm)

Given integers a, b such that $a > 0$, $a < b$ then there exist two unique integers q and r , $0 \leq r < a$ s.t. $b = aq + r$.

Proof:

Uniqueness of q and r :

assume $\exists q'$ and r' s.t $b = aq' + r'$, $0 \leq r' < a$, q' integer

then $aq + r = aq' + r' \Rightarrow a(q - q') = r' - r \Rightarrow q - q' = (r' - r)/a$

as $0 \leq r, r' < a \Rightarrow -a < (r' - r) < a \Rightarrow -1 < (r' - r)/a < 1$

So $-1 < q - q' < 1$, but $q - q'$ is integer, therefore

$q = q'$ and $r = r'$

Prime and Composite Numbers

Definition

An integer $n > 1$ is called a **prime number** if its positive divisors are 1 and n .

Definition

Any integer number $n > 1$ that is not prime, is called a **composite number**.

Example

Prime numbers: 2, 3, 5, 7, 11, 13, 17 ...

Composite numbers: 4, 6, 25, 900, 17778, ...

Decomposition in Product of Primes

Theorem (Fundamental Theorem of Arithmetic)

Any integer number $n > 1$ can be written as a product of prime numbers (>1), and the product is unique if the numbers are written in increasing order.

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$$

Example: $84 = 2^2 \cdot 3 \cdot 7$

Greatest Common Divisor (GCD)

Definition

Given integers $a > 0$ and $b > 0$, we define $\text{gcd}(a, b) = c$, the **greatest common divisor (GCD)**, as the greatest number that divides both a and b .

Example

$$\text{gcd}(256, 100) = 4$$

Definition

Two integers $a > 0$ and $b > 0$ are relatively prime if $\text{gcd}(a, b) = 1$.

Example

25 and 128 are relatively prime.

GCD as a Linear Combination

Theorem

Given integers $a, b > 0$ and $a > b$, then $d = \gcd(a, b)$ is the least positive integer that can be represented as $ax + by$, x, y integer numbers.

Proof: Let t be the smallest positive integer s.t. $t = ax + by$. We have $d \mid a$ and $d \mid b \implies d \mid ax + by$, so $d \mid t$, so $d \leq t$.

We now show $t \leq d$.

First $t \mid a$; otherwise, $a = tu + r$, $0 < r < t$;

$r = a - ut = a - u(ax + by) = a(1 - ux) + b(-uy)$, so we found another linear combination and $r < t$. Contradiction.

Similarly $t \mid b$, so t is a common divisor of a and b , thus $t \leq \gcd(a, b) = d$. So $t = d$.

Example

$$\gcd(100, 36) = 4 = 4 \cdot 100 - 11 \cdot 36 = 400 - 396$$

GCD and Multiplication

Theorem

Given integers $a, b, m > 1$. If
 $\gcd(a, m) = \gcd(b, m) = 1$, then $\gcd(ab, m)$
 $= 1$

Proof idea:

$$ax + ym = 1 = bz + tm$$

Find u and v such that $(ab)u + mv = 1$

GCD and Division

Theorem

Given integers $a > 0$, b , q , r , such that $b = aq + r$, then $\gcd(b, a) = \gcd(a, r)$.

Proof:

Let $\gcd(b, a) = d$ and $\gcd(a, r) = e$, this means

$d \mid b$ and $d \mid a$, so $d \mid b - aq$, so $d \mid r$
Since $\gcd(a, r) = e$, we obtain $d \leq e$.

$e \mid a$ and $e \mid r$, so $e \mid aq + r$, so $e \mid b$,
Since $\gcd(b, a) = d$, we obtain $e \leq d$.

Therefore $d = e$

Finding GCD

Using the Theorem: Given integers $a > 0$, b , q , r , such that $b = aq + r$, then $\gcd(b, a) = \gcd(a, r)$.

Euclidian Algorithm

Find $\gcd(b, a)$

while $a \neq 0$ *do*

$r \leftarrow b \bmod a$

$b \leftarrow a$

$a \leftarrow r$

return b



Euclidian Algorithm Example

Find $\text{gcd}(143, 110)$

$$143 = 1 \square 110 + 33$$

$$110 = 3 \square 33 + 11$$

$$33 = 3 \square 11 + 0$$

$$\text{gcd}(143, 110) = 11$$

Towards Extended Euclidian Algorithm

- **Theorem:** Given integers $a, b > 0$ and $a > b$, then $d = \gcd(a,b)$ is the least positive integer that can be represented as $ax + by$, x, y integer numbers.
- How to find such x and y ?
- Hint: use a modified version of the Euclidian algorithm

Extended Euclidian Algorithm

```
x=1; y=0; d=a; r=0; s=1; t=b;
while (t>0) {
    q = ⌊d/t⌋
    u=x-qr; v=y-qs; w=d-qt
    x=r;    y=s;    d=t
    r=u;    s=v;    t=w
}
return (d, x, y)
```

Invariants:

$$ax + by = d$$

$$ar + bs = t$$

Number of Prime Numbers

Theorem

The number of prime numbers is infinite.

Proof:

consider p_1, p_2, \dots, p_k all primes and $n = p_1 p_2 \dots p_k + 1$.

Then exists p prime s.t. $p \mid n$ (fundamental theorem of arithmetic), and p is not one of the p_1, \dots, p_k (otherwise this will mean that $p \mid 1$).

Therefore, p_1, \dots, p_k were not all the prime numbers.

Distribution of Prime Numbers

Theorem (Gaps between primes)

For every positive integer n , there are n or more consecutive composite numbers.

Proof Idea:

Numbers $(n+1)! + 2, (n+1)! + 3, \dots, (n+1)! + n + 1$ are composite

Distribution of Prime Numbers

Definition

Given real number x , then $\pi(x)$ is the number of prime numbers $\leq x$.

Theorem (prime numbers theorem)

$$\lim_{x \rightarrow \infty} \frac{\pi(x)}{x / \ln x} = 1$$

For a very large number x , the number of prime numbers smaller than x is $x / \ln x$.