CS1800
Discrete Structures
Fall 2017

Lecture 10
9/27/17

Last time

- Finish properties of mod
  - exponentiation
  - add. & mult. identities
  - add. & mult. inverses
- Solving equations (mod n)
  - inverses & linear decryption

Today

- Finish solving equations (mod n)
- divides, division
- primes
- GCD, LCM

Next time

- Euclid's algorithm for GCD
- inverses (mod n)

Check: Is 21 the mult. inv. of 5 $\pmod{26}$

$$21 \cdot 5 \overset{?}{\equiv} 1 \pmod{26}$$

$$105 \overset{?}{\equiv} 1 \pmod{26}$$

$$(4 \cdot 26 + 1) = 1 \pmod{26} \checkmark$$

So,

$$5x = y + 15 \pmod{26}$$

$$21 \cdot 5x = 21(y + 15) \pmod{26}$$

$$x = 21y + 21 \cdot 15 \pmod{26}$$

$$= 21 \cdot y + \underline{21 \cdot 3} \cdot 5 \pmod{26}$$

$$= 21 \cdot y + 63 \cdot 5 \pmod{26}$$

$$= 21 \cdot y + 11 \cdot 5 \pmod{26}$$

$$= 21 \cdot y + 55 \pmod{26}$$

$$= 21 \cdot y + 3$$

Encryt: $y = 5 \cdot x + 11 \pmod{26}$

Decrypt: $x = 21 \cdot y + 3 \pmod{26}$

check

Encryt H → 07 → $(5 \cdot 7 + 11) \bmod 26$

$= (35 + 11) \bmod 26$

$= 46 \bmod 26$

$= 20$

→ U

Decrypt: U → 20 → $(21 \cdot 20 + 3) \bmod 26$

$= (21 \cdot 5 \cdot 4 + 3) \bmod 26$

$= (105 \cdot 4 + 3) \bmod 26$

$= (1 \cdot 4 + 3) \bmod 26$

$= 7$

→ H

Divides

a divides b, denoted $a \mid b$ $\quad b \bmod a = 0$

e.g. $2 \mid 4 \iff 4 \bmod 2 = 0$

a does not divide b, denoted $a \nmid b$ $\quad b \bmod a \neq 0$

e.g. $2 \nmid 5 \iff 5 \bmod 2 \neq 0$

Properties

1. If $a \mid b$ and $a \mid c$ then $a \mid (b+c)$

   e.g. $2 \mid 4$ & $2 \mid 6 \Rightarrow 2 \mid (4+6) \Rightarrow 2 \mid 10$

2. If $a \mid b$ then $a \mid b \cdot c$ $\forall$ integers c

3. If $a \mid b$ & $b \mid c$ then $a \mid c$

Primes

Def: A positive integer $p > 1$ is **prime** if

$\nexists\ k,\ 1 < k < p,$ such that $k \mid p$.

Finding primes: Sieve of Eratosthenes

~~1~~ 2 3 ~~4~~ 5 ~~6~~ 7 ~~8~~ ~~9~~ ~~10~~ 11 ~~12~~ 13 ~~14~~ ~~15~~ ~~16~~ 17 ~~18~~ 19 ~~20~~ ~~21~~

$$x \to x^b \bmod n$$

Theorem: There are infinitely many primes

Proof: Suppose for the sake of contradiction ∃ only a finite # primes. Let

$S = \{ p_1, p_2, p_3, \ldots, p_n \}$. Now consider

$P = p_1 \cdot p_2 \cdot p_3 \cdots p_n + 1$. P is either prime or non-prime (composite).

Case 1: P is prime. Then P must be in S.
But P is bigger than every p_i in S. ✶.

Case 2: P is composite. Then P must be a product of primes in S; i.e., some p_i in S must divide P. But no p_i divides P evenly: always get a remainder of 1. ✶

Thus, claim must be true. (alternative yields contradictions.)

Fundamental theorem of Arithmetic:

Every positive integer has a unique prime factorization.

E.g. $142 = 2 \cdot 71$

$136 = 2 \cdot 68$

$= 2 \cdot 2 \cdot 34$

$= 2 \cdot 2 \cdot 2 \cdot 17$

$= 2^3 \cdot 17$

$96 = \cdots = 2^5 \cdot 3$

GCD = greatest common divisor GCD(12,15) = 3

LCM = least common multiple LCM(12,15) = 60

Def: GCD For a & b, not both 0, the greatest common divisor of a & b, $\gcd(a,b)$, is the largest d s.t. $d|a$ & $d|b$.

Def: LCM For a & b, the least common multiple of a & b is the smallest integer m s.t. $a|m$ & $b|m$

GCD & LCM Examples

$\gcd(12, 15) = 3$

$\gcd(6, 42) = 6$

$\gcd(110, 66) = 22$

$110 = 2 \cdot 5 \cdot 11$

$66 = 2 \cdot 3 \cdot 11$

$\gcd(128, 10931) = 1$

$128 = 2^7$

10931 is odd

$\gcd(289, 10931) = 17$

$289 = 17^2$

$10931 = 17 \cdot 643$

$\gcd(2^2 \cdot 5^2 \cdot 13, 2 \cdot 5^2 \cdot 7) = 2 \cdot 5^2 = 50$

$\gcd(2^2 \cdot 3^2 \cdot 5 \cdot 7^2, 2^2 \cdot 3^4 \cdot 5^2 \cdot 7) = 2^2 \cdot 3^2 \cdot 5 \cdot 7$

CS1800
Discrete Structures
Fall 2017

Lecture 11
9/28/17

Last time

- Finish solving equations (mod n)
  - additive inverses
  - multiplicative inverses
- divides, division
- primes
- GCD, LCM

Today

- GCD, LCM
- Euclid's Alg. for GCD
  - proof
- Inverses mod n
  - Extended Euc. Alg.

Next time

- Finish Ext. Euc.
- Public-Key Crypto.
- RSA

GCD & LCM Examples

$\gcd(12, 15) = 3$

$\gcd(6, 42) = 6$

$\gcd(110, 66) = 22$

$110 = 2 \cdot 5 \cdot 11$

$66 = 2 \cdot 3 \cdot 11$

$\gcd(128, 10931) = 1$

$128 = 2^7$

10931 is odd

$\gcd(289, 10931) = 17$

$289 = 17^2$

$10931 = 17 \cdot 643$

$\gcd(2^2 \cdot 5^2 \cdot 13, 2 \cdot 5^2 \cdot 7) = 2 \cdot 5^2 = 50$

$\gcd(2^2 \cdot 3^2 \cdot 5 \cdot 7^2, 2^2 \cdot 3^4 \cdot 5^2 \cdot 7) = 2^2 \cdot 3^2 \cdot 5 \cdot 7$

$\gcd(p_1^{e_1} \cdot p_2^{e_2} \cdots p_n^{e_n}, p_1^{f_1} p_2^{f_2} \cdots p_n^{f_n}) = p_1^{\min(e_1, f_1)} \cdots p_n^{\min(e_n, f_n)}$

LCM: least common multiple

$\text{lcm}(12,15) = \text{lcm}(2^2 \cdot 3, 3 \cdot 5) = 2^2 \cdot 3 \cdot 5 = 4 \cdot 3 \cdot 5 = 60$

$\text{lcm}(2^5 \cdot 3^2 \cdot 5 \cdot 7^2, 2^2 \cdot 3^4 \cdot 5^2 \cdot 7) = 2^5 \cdot 3^4 \cdot 5^2 \cdot 7^2$

$\text{lcm}(p_1^{e_1} p_2^{e_2} \cdots p_n^{e_n}, p_1^{f_1} \cdots p_n^{f_n}) = p_1^{\max(e_1,f_1)} \cdots p_n^{\max(e_n,f_n)}$

Claim: $a \cdot b = \gcd(a,b) \cdot \text{lcm}(a,b)$

red green

$a = 2^5 \cdot 3^2 \cdot 5 \cdot 7^2$

$b = 2^2 \cdot 3^4 \cdot 5^2 \cdot 7$

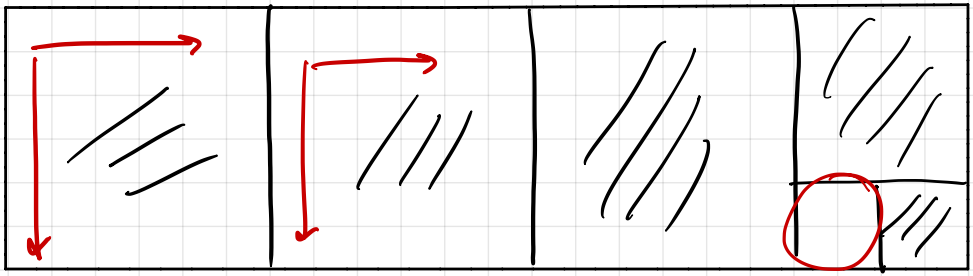
$a \cdot b = 2^5 2^2 \cdot 3^2 3^4 \cdot 5 \cdot 5^2 \cdot 7^2 \cdot 7$

Utility! If GCD (or LCM) is known, then can easily compute other, e.g.,

$$\text{lcm}(a,b) = \frac{a \cdot b}{\gcd(a,b)}$$

claim:
can tile an a×b space evenly w/ d×d tiles iff d is a common factor of a & b.

largest such d×d tile is gcd(a,b)



6

$a \geq b$ $\quad \gcd(a,b) = \gcd(a-b,b)$

$= \gcd(a-2b,b)$

$= \gcd(a-3b,b)$

$\vdots$

$= \gcd(a-q\cdot b,b)$ where $a = q\cdot b + r$

$= \gcd(a \bmod b, b)$

$$\boxed{\gcd(a,b) = \gcd(b, a \bmod b)}$$

e.g. $\gcd(22,6) = \gcd(6, 22 \bmod 6) = \gcd(6,4)$

$\gcd(22,6) = \gcd(22-6,6)$

$= \gcd(16,6)$

$= \gcd(10,6)$

$= \gcd(4,6)$

$= \gcd(6,4)$

$= \gcd(2,4)$

$= \gcd(4,2)$

$= \gcd(2,2)$

$= 2$

Thm: $a \geq b$, $\gcd(a,b) = \gcd(a-b, b)$

Pf: g is a common factor of a & b

iff g is a common factor of $a-b$ & b

$\Rightarrow$ g is common factor of a & b

$g \mid a$ & $g \mid b$

$a = c_1 \cdot g$, $b = c_2 \cdot g$ for some int. c_1 & c_2, $c_1 \geq c_2$

$$a - b = c_1 \cdot g - c_2 \cdot g$$
$$= (c_1 - c_2) \cdot g$$
$$= c_3 \cdot g \quad \text{for } c_3 = c_1 - c_2$$

So, $g \mid (a-b)$ (and $g \mid b$)

$\Leftarrow$ $g \mid (a-b)$ & $g \mid b$

$a - b = c_4 \cdot g$ $\quad b = c_2 \cdot g$

$a - c_2 \cdot g = c_4 \cdot g \iff a = c_2 \cdot g + c_4 \cdot g$ So, $g \mid a$ (and $g \mid b$)

$= (c_2 + c_4) \cdot g$

Thm: $a \geq b$, $\gcd(a,b) = \gcd(b, a \bmod b)$

Pf: Let $a = q \cdot b + r$ by division alg.
where $r = a \bmod b$

Then
$$\begin{aligned}
\gcd(a,b) &= \gcd(a-b, b) && \text{(prev thm)} \\
&= \gcd(a-2b, b) && \text{"} \\
&\vdots \\
&= \gcd(a-q\cdot b, b) \\
&= \gcd(r, b) \\
&= \gcd(a \bmod b, b) \quad \checkmark
\end{aligned}$$