Modular Arithmetic

+ finishing primes

Discrete Mathematics

Courtesy of Andrei Bulatov

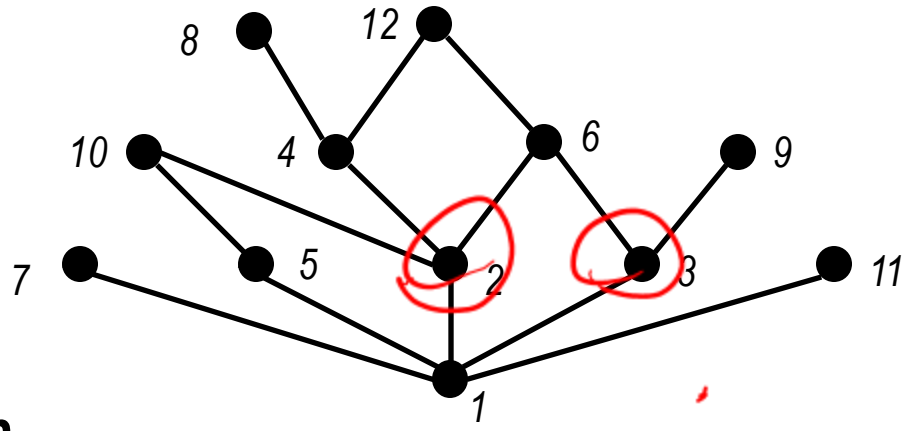
Previous Lecture

- *Divisors, properties of divisibility*
- *Greatest common divisor*
- *Euclidean algorithm*

Least Common Multiple

- *A positive integer c is called a common multiple of integers a and b if a | c and b | c*

- *The number c is called the least common multiple of a and b, denoted lcm(a,b) if it is a common multiple and for any common multiple d we have c | d*



- **Theorem.**
  For any integers a and b, the least common multiple exists.

Least Common Multiple (cntd)

- **Theorem**

  For any integers a and b we have $ab = lcm(a,b) \cdot gcd(a,b)$

Example:

Find lcm(15,21).

$21 = 1 \cdot 15 + 6$

$15 = 2 \cdot 6 + 3$

$6 = 2 \cdot 3 + 0$

$15 \cdot 21 = 315$

$315 / 3 = 105$

The Fundamental Theorem of Arithmetic

- **Theorem**.

  Every integer $n > 1$ can be represented uniquely as a product of primes, up to the order of the primes, called its prime factorization.

- **Proof** *(Existence)*

  Base case: 2 is prime so it is a product of primes

  Inductive step:

  Assume every integer $2 \le i \le k$ has a prime factorization

  Now consider the integer k+1

  If k+1 is prime, we're done

  If k+1 is not prime, then $k+1=ab$ where $1 < a,b < k+1$

  By the inductive hypothesis, a and b have prime factorizations

  So k+1 also has a prime factorization *Q.E.D*

Example

- *Find the prime factorization of 4270*

$$4270 = 4200 + 70$$
$$= 7 \cdot 600 + 7 \cdot 10$$
$$= 7 \cdot 2 \cdot (300 + 5)$$
$$= 7 \cdot 2 \cdot 5 \cdot 61$$

Uniqueness of prime decomposition

- *To prove uniqueness of the prime factorization, need a lemma*

- *Lemma:*
  Let a_i be an integer for $1 \le i \le n$, and suppose p is a prime such that $p \mid a_1 a_2 \ldots a_n$. Then $p \mid a_i$ for some $1 \le i \le n$.

- *Proof of uniqueness:*
  Suppose $n = p_1 \ldots p_k = q_1 \ldots q_m$ are distinct prime factorizations of n
  WLOG assume there are no common primes, i.e. $\forall i,j\ p_i \neq q_j$
  Then $p_1 \mid p_1 \ldots p_k = q_1 \ldots q_m$, so by the lemma there exists j such that $p_1 \mid q_j$
  But q_j is prime and $q_j \neq p_1$, so we have a contradiction

Relatively Prime

- *Numbers a and b such that gcd(a,b) = 1 are called relatively prime*
- *How many relatively prime numbers are there?*
- *Euler's totient function φ(n) is the number of numbers k such that 0 < k < n and n and k are relatively prime.*
- *If p is prime then every k < p is relatively prime with p. Hence, φ(p) = p – 1.*
- **Lemma**.

  If a and b are relatively prime then φ(ab) = φ(a) · φ(b)
- **Corollary**.

  If $n = p_1^{s_1} p_2^{s_2} \ldots p_u^{s_u}$ *is the prime factorization of n, then*

$$\varphi(n) = n \cdot \left(1 - \frac{1}{p_1}\right)^{s_1} \left(1 - \frac{1}{p_2}\right)^{s_2} \cdots \left(1 - \frac{1}{p_u}\right)^{s_u}$$

Congruences

- *In some situations, we care only about the remainder of an integer when it is divided by some number.*
  - *If I bake 79 cookies, how many more do I need to make to sell them in even dozens?*
- *Congruence modulo m classifies numbers by their remainder when divided by m*
- *Definition:*

  a and b are congruent modulo m if and only if $m \mid (a - b)$
- *We use the notation $a \equiv b \pmod{m}$ to denote a, b congruent modulo m*
- *Fact:*

  $a \equiv b \pmod{m}$ *if and only if* $a = q_1 m + r$ *and* $b = q_2 m + r$

  same remainder

Congruences (cntd)

- *Examples:*

  $12 \equiv 5 \pmod 7$

  $12 \equiv 6 \pmod 3$

  $12 \equiv -3 \pmod{15}$

  $12 \equiv 0 \pmod{12}$

- *Theorem:*

  For any integers a, b, and m, $a \equiv b \pmod m$ if and only if $a = b + km$ for some integer k.

Proof:

By definition, $a \equiv b \pmod m$ if and only if $a - b = km$ for some integer k. Then $a = b + km$

Congruences and Arithmetic Operations

- *Addition, subtraction, multiplication behave really well with respect to congruences*

- **Theorem**.
  Let m be positive integer. If $a \equiv b \pmod m$ and $c \equiv d \pmod m$, then
  (1) $a + c \equiv b + d \pmod m$,
  (2) $a - c \equiv b - d \pmod m$, and
  (3) $ac \equiv bd \pmod m$

- *Proof sketch*
  (3) Let $a = b + km$ and $c = d + lm$ for some k and l.
  Then $ac = (b + km)(d + lm) = bd + blm + dkm + klm$
  $= bd + (bl + dk + klm)m$

Example

- *7+11 (mod 5)*

$7 \equiv 2 \pmod 5$

$11 \equiv 1 \pmod 5$

$7+11 = 18 \equiv 3 \pmod 5$

$7+11 \equiv 2+1 \pmod 5$

$\equiv 3 \pmod 5$

- *743*987654 (mod 5)*

$743 \equiv 3 \pmod 5$

$987654 \equiv 4 \pmod 5$

$743 \cdot 987654 \equiv 3 \cdot 4 \pmod 5$

$\equiv 2 \pmod 5$

Congruences and Arithmetic Operations (cntd)

- *Division is not so good:*

  Although $8 \equiv 24 \pmod 4$ *and* $4 \equiv 8 \pmod 4$,

  $$\frac{8}{4} = 2 \not\equiv 3 = \frac{24}{8} \pmod 4$$

Residues

- *Let us consider the binary relation $\equiv$ modulo m on the set of integers, that is,*

$$\{(a,b) \mid a \equiv b \pmod{m}\}$$

- *It is reflexive, symmetric, and transitive. This is an equivalence relation*

- *Each such relation defines a partition on the set of integers into equivalence classes*

$$[a \bmod m] = \{ b \mid a \equiv b \pmod{m}\}$$

- *We choose a canonical representative for each such class, which is the (unique) residue of a modulo m*

Residues (cntd)

- *The residue of an integer a modulo m is such a number b that* $a \equiv b \pmod{m}$ *and* $0 \leq b < m$
- *In other words the residue of a modulo m is the remainder of a when divided by m*
- *Let* $\mathbb{Z}_m$ *denote the set* $\{0,1,2,\ldots,m-1\}$. *This is the set of all possible remainders of integers when divided by m*
- *It is called the set of residues, and its members are called residues*

Modular Arithmetic

- *We define addition, subtraction, and multiplication of residues:*

  Let $a,b \in \mathbb{Z}_m$. *Then*

  $a + b \pmod m$ *is the element* $c \in \mathbb{Z}_m$ *such that* $c \equiv a + b \pmod m$

  $a - b \pmod m$ *is the element* $c \in \mathbb{Z}_m$ *such that* $c \equiv a - b \pmod m$

  $a \cdot b \pmod m$ *is the element* $c \in \mathbb{Z}_m$ *such that* $c \equiv a \cdot b \pmod m$

- *Example. Construct operation tables for* $\mathbb{Z}_5$

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

·	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Divisors of Zero

- *Modular addition just rotates/shifts/cycles the numbers*
  - *In particular, it* **is injective as a function** $f(x) = x + a \pmod m$
- *Multiplication however is not injective*

·	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

- *A proper 0 divisor modulo m is a residue* $a \not\equiv 0 \pmod m$ *such that there exists* $b \not\equiv 0 \pmod m$ *with* $a \cdot b \equiv 0 \pmod m$.
- $\mathbb{Z}_4$ *has a proper 0 divisor.* $\mathbb{Z}_5$ *does not.*

Inverse

- *A residue b modulo m is called an inverse of a residue a if $a \cdot b \equiv 1 \pmod{m}$, denoted a^{-1}*
- *3 is the inverse of 2 modulo 5*
- *2 does not have an inverse modulo 4*
- **Theorem**

  Let a be residue modulo m. The following conditions are equivalent:

  (i) a has an inverse;

  (ii) a is not a proper divisor of 0;

  (iii) a is relatively prime with m.

Inverse (cntd)

- **Proof**.

  (i) $\Rightarrow$ (ii) By contradiction.

  Suppose $a \cdot b \equiv 0 \pmod m$ for some b not equal to 0.

  Then $a^{-1} \cdot a \cdot b \equiv a^{-1} \cdot 0 \pmod m$

  $b \equiv 1 \cdot b \equiv 0 \pmod m$, a contradiction

  (ii) $\Rightarrow$ (iii) By contraposition.

  Suppose $\gcd(a,m) = d$ and $a = ld$, $m = kd$.

  Then $ak \equiv kld \equiv lm \equiv 0 \pmod m$.

  Thus a is a proper divisor of 0.

  (iii) $\Rightarrow$ (i)

  Suppose $\gcd(a,m) = 1$. Then there are u,v with $au + mv = 1$.

  Thus $au \equiv 1 \pmod m$; a has an inverse.

Practice

Exercises from the Book:

7th edition: 28, 35, 40 (page 245), 5, 17 (page 284 – 285)

8th edition: 34, 41, 46 (page 259), 5, 17 (page 301)