Number Theory, Sets

June 24, 2014

Yesterday

$$7^{100} \bmod 11 = 1.$$

In fact $2^{100} \bmod 11, 3^{100} \bmod 11, \ldots, 10^{100} \bmod 11$ are all 1.

Modular arithmetic example

Proposition

If n is odd, then $n^2 \equiv 1 \pmod 8$.

Proof: Let $r = n \bmod 8$. Since $n = 8q + r$ for some q, r is odd. By the above proposition, $n^2 \equiv r^2 \pmod 8$. Now look at cases.

Inverses

Corollary (*)

Two positive integers a and b are relatively prime if and only if there exist integers s and t such that $sa + tb = 1$.

Proof: You've already seen this.

Theorem

If a and m are positive integers, then there exists a positive integer b such that $ab \equiv 1 \pmod{m}$ if and only if $\gcd(a, m) = 1$.

Proof: Use above proposition.

Definition

In the above, b is the **modulo** m **multiplicative inverse** of a.

Inverses

Theorem

If a and m are positive integers, then there exists a positive integer b such that $ab \equiv 1 \pmod{m}$ if and only if $\gcd(a, m) = 1$.

Corollary

If a and p are positive integers, p is prime, and $p \nmid a$, then there exists a positive integer b such that $ab \equiv 1 \pmod{p}$.

Example: If we have the congruence $xy \equiv xz \pmod{m}$ and $m \nmid x$, then $y \equiv z \pmod{m}$.
How do we find the inverse?

Theorem

If a is an integer, p is prime, and $p \nmid a$, then the numbers $0, a \bmod p, 2a \bmod p, \ldots, (p-1)a \bmod p$ are all different.

Example: If $a = 3$ and $p = 7$, then $(0, a \bmod p, ..., (p-1)a \bmod p) = (0, 3, 6, 2, 5, 1, 4)$

Fermat's Little Theorem

Theorem (Fermat's Theorem)

If a is an integer, p is prime, and $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$.

Example: $4^6 \equiv 1 \pmod{7}$, since $4^6 = 4096 = 7 \times 585 + 1$.

Corollary

Modulo p, a^{p-2} is a multiplicative inverse of a.

Euler's totient function

Definition

If n is a positive integer, then $\phi(n)$ is the number of positive integers that are less than n and relatively prime to n.

Example: $\phi(7) = 6$, $\phi(12) = 4$.

Corollary

If p is prime, then $\phi(p) = p - 1$.

Theorem

If p is a prime and k is a positive integer, then $\phi(p^k) = p^k - p^{k-1} = (1 - \frac{1}{p})p^k$.

More about ϕ

Definition

If n is a positive integer, then $\phi(n)$ is the number of positive integers that are less than n and relatively prime to n.

Theorem

If m and n are positive integers and relatively prime, then $\phi(mn) = \phi(m)\phi(n)$.

Example: $\phi(300) = \phi(2^2)\phi(3)\phi(5^2) = 2 \cdot 2 \cdot 20 = 80$.
In particular, if p and q are primes, then $\phi(pq) = (p-1)(q-1)$.

Euler's Generalization

Theorem

If a and m are positive integers, then there exists a positive integer b such that $ab \equiv 1 \pmod{m}$ if and only if $\gcd(a, m) = 1$.

Theorem

If a and n are integers and $\gcd(a, n) = 1$, then $a^{\phi(n)} \equiv 1 \pmod{n}$.

Corollary

If a and n are integers and $\gcd(a, n) = 1$, then $a^{\phi(n)-1}$ is the multiplicative inverse of a.

Cryptography

- Alice wants to send a message m to Bob.
- Alice encrypts her message to $E(m)$ and sends it.
- Bob decrypts her message to $D(E(m))$.

Problems:

- We need $D(E(m)) = m$.
- Alice and Bob need to agree on E and D
- Nobody else can know D.

Public key cryptography

Solution:

- Bob generates E and D by himself.
- He designs E and D such that D is difficult to figure out from E but $E(D(m)) = m$ anyway.
- He keeps D for himself, but sends E to everyone in the world, including Alice.
- D is called the **private key**, and E the **public key**.

RSA

1. Bob generates two distinct primes p and q.
2. Let $n = pq$.
3. Bob selects an integer e such that $\gcd(e, (p-1)(q-1)) = 1$. The public key is (e, n).
4. Bob computes d such that $de \equiv 1 \pmod{(p-1)(q-1)}$. The private key is (d, n)

Encryption: If the plaintext is m and $m < n$, then the sender sends

$$m' = m^e \bmod n.$$

Decryption: If the ciphertext is m', then the receiver computes

$$m'' = (m')^d \bmod n.$$

RSA, Correctness

We need to show that the receiver's decrypted message is the same as the sender's plaintext.

Theorem

If d, e, m, n are all positive integers such that $de \equiv 1 \pmod{(p-1)(q-1)}$, then

$$m = m^{ed} \bmod n = (m^e \bmod n)^d \bmod n$$

Is RSA safe?

- The public key is (e, n), where $n = pq$, and the private key is (d, n).
- If we can find p and q, then we can use Euler's theorem to find d and thus break RSA.
- Factoring numbers on a classical computer efficiently is an unsolved problem.
- Shor's algorithm runs on a quantum computer and can factor numbers efficiently.
- As of 2012, the largest number a quantum computer has factored is 143 (it did not use Shor's algorithm).

Unfortunate quote

“No one has yet discovered any warlike purpose to be served by the theory of numbers or relativity, and it seems unlikely that anyone will do so for many years.” - G. H. Hardy, 1940

Sets

Definition

A **set** is an unordered collection of distinct objects. These objects are **elements** of the set.

- Elements can be anything: numbers, points, shapes, people, ...
- The **universe** is the set of all things you might put in the set (e.g., all integers, or all reals).
- "unordered": A set containing the numbers 1 and 2 is the same as the one containing 2 and 1.
- "distinct": A set cannot repeat objects.

Basics of sets

- To write a set, we can just list the elements.
- We can also use letters to denote sets.
- Example: $S = \{3, 5, 7\}$
- $x \in A$ means that x is an element of A.
- In the above example, $3 \in S$.

Definition

The **empty set** does not contain any elements and is denoted $\{\}$ or $\emptyset$.

Set-builder notation

- Example: $\{x \in \mathbb{R} \mid 3 \leq x \leq 7\}$
- Read "The set of all real numbers x such that $3 \leq x \leq 7$."
- Equivalent to $\{x \mid x \in \mathbb{R} \wedge 3 \leq x \leq 7\}$
- "The set of all x such that x is a real number and $3 \leq x \leq 7$."

Set operations

- Intersection: $A \cap B = \{x \mid x \in A \wedge x \in B\}$
- Union: $A \cap B = \{x \mid x \in A \vee x \in B\}$
- Difference: $A \setminus B = A - B = \{x \mid x \in A \wedge x \notin B\}$
- Complement: $\bar{A} = U - A = \{x \mid x \in U \wedge x \notin A\}$
- Cartesian Product: $A \times B = \{(a, b) \mid a \in A \wedge b \in B\}$

Set operations example

Example: If $A = \{2, 3, 4\}$ and $B = \{2, 4, 7\}$, then

- $A \cap B = \{2, 4\}$
- $A \cup B = \{2, 3, 4, 7\}$
- $A - B = \{3\}$
- $A \times B = \{(2,2),(2,4),(2,7),(3,2),(3,4),(3,7),(4,2),(4,4),(4,7)\}$.
- What is $\bar{A}$?

Sizes of sets

The **size** of a set A is the number of elements A has and is denoted $|A|$.
Example: If $A = \{1, 3, 99, 432\}$, then $|A| = 4$.

Product Rule

If A and B are sets, then

$$|A \times B| = |A| \times |B|$$

Example: In a non-standard deck of cards, there are 3 suits and 18 ranks. How many cards are there?
Example: How many four-digit positive integers are there whose digits are either 3, 4, or 5?

Complementary Counting

If A is a set and U is the universe, then

$$|A| = |U| - |\overline{A}|$$

Sometimes it's easier to calculate $|\overline{A}|$.
Example: How many four-digit positive integers have at least one digit that is a 2 or a 3?

Principle of Inclusion-Exclusion (PIE)

Theorem

If A, B, and C are sets, then

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|.$$

Proof: Draw a Venn diagram.
What about $|A \cup B \cup C \cup D|$, etc.?