MA/CSSE 473 Day 09

Modular Division Revisited

Fermat's Little Theorem

Primality Testing

MA/CSSE 473 Day 09

- Trominoes implementation due tomorrow at 8 AM.
- HW 5 due Tuesday
- A "late day" ends 24 hours after the assignment is due. Submit whatever you have done before that time.
- **Student Question from previous quiz**
  - Why are we doing all this modular stuff?
- Modular inverse, division revisited
- Fermat's Little Theorem proof
- Primality Testing

My concern…

Recap: Extended Euclid Algorithm

- Given positive integers a and b
- Extended Euclid algorithm returns integers x, y, d, such that
  - d = gcd(a, b)
  - d = ax + by
- We use this as the basis for calculating modular inverse

Another place to read about modular arithmetic, including exponentiation and inverse: Weiss Sections 7.4-7.4.4

Revisit: Modular Inverse

- In arithmetic over the real or rational numbers, every non-zero number **a** has an inverse 1/**a**.
- **Definition** x is the **multiplicative inverse of** a **modulo** N if **a**x ≡ 1 (mod N)
- We denote this inverse by $\mathbf{a}^{-1}$ (if it exists)
  - Note that 2 has no inverse modulo 6
  - **a** has an inverse modulo N if and only if gcd(a, N) = 1
    - i.e. **a** and N are **relatively prime**
- If $\mathbf{a}^{-1}$ exists, it is unique (among 1..N-1)

Calculate Modular Inverse (if it exists)

- Assume that gcd(a, N) = 1.
- The extended Euclid's algorithm gives us integers x and y such that ax + Ny = 1
- This implies $ax \equiv 1 \pmod{N}$, so x is the inverse of a
- **Example:** Find $11^{-1} \bmod 25$
  - We saw before that -34*11 + 15*25 = 1
  - $-34 \equiv 16 \pmod{25}$
  - So $11^{-1} = 16 \bmod 25$
- Recall that Euclid's algorithm is $\Theta(n^3)$, where n is the number of bits of N.

Revisit: Modular division

- We can only divide b by a (modulo N) if N and a are relatively prime
- In that case b/a is defined to be $b \cdot a^{-1}$
- What is the running time for modular division?

Recap: Fermat's Little Theorem

- **Formulation 1:** If p is prime, then for every number a with $1 \le a < p$, $a^{p-1} \equiv 1 \pmod{p}$
- **Formulation 2:** If p is prime, then for every number a with $1 \le a < p$, $a^{p} \equiv a \pmod{p}$
- These are clearly equivalent.
  - How do we get from each to the other?
- We will examine a combinatorial proof of the first formulation.

Fermat's Little Theorem: Proof (part 1)

- **Formulation 1:** If **p** is prime, then for every number **a** with $1 \le \mathbf{a} < \mathbf{p}$, $\mathbf{a}^{\mathbf{p}-1} \equiv 1 \pmod{\mathbf{p}}$
- Let S = {1, 2, …, **p**-1}
- **Lemma**
  - Multiplying all of the numbers in S by **a** (mod **p**) permutes S
  - I.e. $\{a \cdot n \pmod{p} : n \in S\} = S$
- **Example:** **p**=7, a=3.

k	1	2	3	4	5	6
3k	3	6	2	5	1	4

- **Proof of the lemma**
  - Suppose that $\mathbf{a} \cdot i \equiv \mathbf{a} \cdot j \pmod{\mathbf{p}}$.
  - Since **p** is prime and $\mathbf{a} \neq 0$, **a** has an inverse.
  - Multiplying both sides by $\mathbf{a}^{-1}$ yields $i \equiv j \pmod{\mathbf{p}}$.
  - Thus, multiplying the elements of S by **a** (mod **p**) takes each element to a different element of S.
  - Thus (by the pigeonhole principle), every number 1..**p**-1 is $\mathbf{a} \cdot i \pmod{\mathbf{p}}$ for some i in S.

Fermat's Little Theorem: Proof (part 2)

- **Formulation 1:** If **p** is prime, then for every number **a** with
  $1 \le \mathbf{a} < p$, $\mathbf{a}^{\mathbf{p}-1} \equiv 1 \pmod{\mathbf{p}}$
- Let S = {1, 2, …, **p**-1}
- **Lemma** Multiplying all of the numbers in S by **a** (mod **p**) permutes S
- **Therefore:**
  {1, 2, …, **p**-1} = {**a**·1 mod **p**, **a**·2 mod **p**, … **a**·(**p**-1) mod **p**}
- Take the product of all of the elements on each side .
  $(\mathbf{p}-1)! \equiv \mathbf{a}^{\mathbf{p}-1}(\mathbf{p}-1)! \pmod{\mathbf{p}}$
- Since **p** is prime, (**p**-1)! is relatively prime to **p**, so we can divide both sides by it to get the desired result.

Easy Primality Test?

- Is N prime?
- Pick some **a** with $1 < \mathbf{a} < N$
- Is $\mathbf{a}^{N-1} \equiv 1 \pmod{N}$?
- If so, N is prime; if not, N is composite
- But, wait a minute!
  - Fermat's Little Theorem is not an "if and only if" condition.
  - It doesn't say what happens when N is not prime.
  - N may not be prime, but we might just happen to pick an **a** for which $\mathbf{a}^{N-1} \equiv 1 \pmod{N}$
  - **Example:** 341 is not prime (it is 11·31), but $\mathbf{2}^{340} \equiv 1 \pmod{341}$
- **Definition:** We say that a number **a** **passes the Fermat test** if $\mathbf{a}^{N-1} \equiv 1 \pmod{N}$
- We can hope that if N is composite, then many values of **a** will fail the test
- It turns out that this hope is well-founded

"composite" means "not prime"

How many "false positives"?

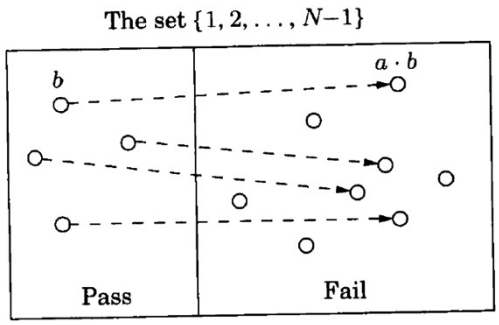
- If N is composite, and we randomly pick an **a** with $1 \le \mathbf{a} < N$, and gcd(a,N) = 1, how likely is it that $\mathbf{a}^{N-1}$ is $\equiv 1 \pmod{n}$?
- If $\mathbf{a}^{N-1} \equiv 1 \pmod{n}$ for *some* **a** that is relatively prime to N, then this must also be true for at least half of the choices of $\mathbf{a} < N$.
  - Let b be some number (if any exist) that passes the Fermat test, i.e. $b^{N-1} \equiv 1 \pmod{N}$.
  - Then the number a·b fails the test:
    - $(ab)^{N-1} \equiv a^{N-1}b^{N-1} \equiv a^{N-1}$, which is not congruent to 1 mod N.
  - Diagram on whiteboard.
  - For a fixed **a**, f: b→ab is a one-to-one function on the set of b's that pass the Fermat test,
  - so there are at least as many numbers that fail the Fermat test as pass it.

Lemma *If $a^{N-1} \not\equiv 1 \bmod N$ for some a relatively prime to N, then it must hold for at least half the choices of $a < N$.*

Proof. Fix some value of a for which $a^{N-1} \not\equiv 1 \bmod N$. The key is to notice that every element $b < N$ that passes Fermat's test with respect to N (that is, $b^{N-1} \equiv 1 \bmod N$) has a twin, $a \cdot b$, that fails the test:

$$(a \cdot b)^{N-1} \equiv a^{N-1} \cdot b^{N-1} \equiv a^{N-1} \not\equiv 1 \bmod N.$$

Moreover, all these elements $a \cdot b$, for fixed a but different choices of b, are distinct, for the same reason $a \cdot i \not\equiv a \cdot j$ in the proof of Fermat's test: just divide by a.



The one-to-one function $b \mapsto a \cdot b$ shows that at least as many elements fail the test as pass it. ∎

Carmichael Numbers

- A Carmichael N number is a composite number that passes the Fermat test for all **a** with 0< **a**<N and gcd(a, N)=1.
  - The smallest Carmichael number is 561
  - We'll see later how to deal with those
  - How rare are they? Let C(X) = number of Carmichael numbers that are less than X.

n	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
$C(10^n)$	1	7	16	43	105	255	646	1547	3605	8241	19279	44706	105212	246683	585355	1401644	3381806	8220777

  - For now, we pretend that we live in a Carmichael-free world

Where are we now?

- We ignore Carmichael numbers for now.
- If N is prime, $a^{N-1} \equiv 1 \pmod{N}$ for all 0< a < N
- If N is not prime, then $a^{N-1} \equiv 1 \pmod{N}$ for at most half of the values of a<N.
- Pr(algorithm returns **true** if N is prime) = 1
  Pr(algorithm returns **true** if N is composite) ≤ ½
- How to reduce the probability of error?