

MA/CSSE 473

Day 09

Modular Division

Primality Testing



MA/CSSE 473 Day 09

- HW 4 is due tomorrow.
- Exam 1: Tuesday, September 30.
 - You may bring your textbook, plus a one-sided 8.5x11 inch piece of paper containing anything that you can read unaided or with normal eyeglasses.
- **Student Questions.**
- Extended Euclid Algorithm example
- Modular Division
- Primality Testing
- Fermat's little theorem



Recap: Extended Euclid Algorithm

```
def euclidExtended(a, b):  
    """ INPUT: Two integers a and b with  $a \geq b \geq 0$   
        OUTPUT: Integers  $x, y, d$  such that  $d = \text{gcd}(a, b)$   
            and  $d = ax + by$  """  
    print "    ", a, b  
    if b == 0:  
        return 1, 0, a  
    x, y, d = euclidExtended(b, a % b)  
    return y, x - a/b*y, d
```



Example: gcd (25, 11)

- $25 = 2 * 11 + 3$
- $11 = 3 * 3 + 2$
- $3 = 1 * 2 + 1$
- $2 = 2 * 1 + 0$, so $\text{gcd}(11, 25) = 1$.
- **Now work backwards**
- $1 = 1 - 0$. Substitute $0 = 2 - 2 * 1$
- $1 = 1 - (2 - 2 * 1) = -1 * 2 + 3 * 1$. Substitute $1 = 3 - 1 * 2$
- $1 = -1 * 2 + 3(3 - 1 * 2) = 3 * 3 - 4 * 2$. Substitute $2 = 11 - 3 * 3$
- $1 = 3 * 3 - 4 * (11 - 3 * 3) = -4 * 11 + 15 * 3$. Substitute $3 = 25 - 2 * 11$
- $1 = -4(11) + 15(25 - 2 * 11) = -34 * 11 + 15 * 25$
- Thus $x = 15$ and $y = -34$ **Done!**



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 $ax \equiv 1 \pmod{N}$.
- We denote this inverse a^{-1} (if it exists)
- 2 has no inverse modulo 6
- In general, a has an inverse modulo N if and only if $\gcd(a, N) = 1$ (i.e. a and N are **relatively prime**)
- If a^{-1} exists, it is unique



Finding the Modular Inverse

- 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 $11^{-1} \pmod{25}$
 - We saw before that $-34 \cdot 11 + 15 \cdot 25 = 1$
 - $-34 \equiv 16 \pmod{25}$
 - So $11^{-1} = 16 \pmod{25}$
- Recall that Euclid's algorithm is $\Theta(n^3)$, where n is the number of bits of N .



Modular division

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



Primality testing

- The numbers 7, 17, 19, 71, and 79 are primes, but what about 717197179 (a typical social security number)?
- There are some tricks that might help. For example:
 - If n is even and not equal to 2, it's not prime
 - n is divisible by 3 **iff** the sum of its decimal digits add is divisible by 3,
 - n is divisible by 5 **iff** it ends in 5 or 0
 - n is divisible by 7 **iff** $\lfloor n/10 \rfloor - 2*n\%10$ is divisible by 7
 - when checking for factors, we only need to consider prime numbers as candidates
 - When checking for factors, we only need to look for numbers up to \sqrt{n}
- But this approach is not very fast. Factoring is much harder than primality testing.
- Is there a way to tell whether a number is prime without actually factoring the number?

Like much of what we have done so far in this course, this discussion follows Dasgupta, *et. al.*, *Algorithms* (McGraw-Hill 2008)



Fermat's Little Theorem (1640)

- **Formulation 1:** If p is prime, then for every number a with $1 \leq a < p$, $a^{p-1} \equiv 1 \pmod{p}$
- **Formulation 2:** If p is prime, then for every number a with $1 \leq a < p$, $a^p \equiv a \pmod{p}$
- These are clearly equivalent.
- 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 $1 \leq a < p$, $a^{p-1} \equiv 1 \pmod{p}$
- Let $S = \{1, 2, \dots, p-1\}$
- **Lemma**
 - Multiplying all of the numbers in S by $a \pmod{p}$ permutes S
- **Example:** $a=3, p=7$
 - $1 \rightarrow 3 \rightarrow 2 \rightarrow 6 \rightarrow 4 \rightarrow 5 \rightarrow 1$
- **Proof of the lemma**
 - Suppose that $a \cdot i \equiv a \cdot j \pmod{p}$.
 - Since p is prime and $a \neq 0$, a has an inverse.
 - Multiplying both sides by a^{-1} yields $i \equiv j \pmod{p}$.
 - Thus, multiplying the elements of S by $a \pmod{p}$ takes each element to a different element of S .
 - Thus (by the pigeonhole principle), every number $1..p-1$ is $a \cdot i \pmod{p}$ for some i in S .

