Spring 2015
Lecture 13: Primes, GCDs, modular inverses

ARE YOU DOING MATH PROBLEMS FOR FUN?

YEAH. I LOVE BEING MENTALLY CHALLENGED.

WELL I'M GLAD YOU'VE COME TO TERMS WITH IT.

THANKS!
Since \( a \mod m \equiv a \pmod m \) for any \( a \)

we have \( a^2 \mod m = (a \mod m)^2 \pmod m \)

and \( a^4 \mod m = (a^2 \mod m)^2 \pmod m \)

and \( a^8 \mod m = (a^4 \mod m)^2 \pmod m \)

and \( a^{16} \mod m = (a^8 \mod m)^2 \pmod m \)

and \( a^{32} \mod m = (a^{16} \mod m)^2 \pmod m \)

Can compute \( a^k \mod m \) for \( k = 2^i \) in only \( i \) steps
ModPow(a, k, m) should compute $a^k \mod m$.

If $k == 0$ then

return 1

If $(k \mod 2 == 0)$ then

return $\text{ModPow}(a^2 \mod m, k/2, m)$

else

return $(a \times \text{ModPow}(a, k - 1, m)) \mod m$

$k = 81453$

$= (10011111000101101)_2$

$= 2^{16} + 2^{13} + 2^{12} + 2^{11} + 2^{10} + 2^9 + 2^5 + 2^3 + 2^2 + 2^0$

Total # of arithmetic operations $\sim 4 \times 16 = 64$
An integer $p$ greater than 1 is called prime if the only positive factors of $p$ are 1 and $p$.

$$p = 13$$

A positive integer that is greater than 1 and is not prime is called composite.

$$26 = 13 \times 2$$
An integer $p$ greater than 1 is called *prime* if the only positive factors of $p$ are 1 and $p$.

A positive integer that is greater than 1 and is not prime is called *composite*. 
Every positive integer greater than 1 has a unique prime factorization

\[
\begin{align*}
48 & = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 \\
591 & = 3 \cdot 197 \\
45,523 & = 45,523 \\
321,950 & = 2 \cdot 5 \cdot 5 \cdot 47 \cdot 137 \\
1,234,567,890 & = 2 \cdot 3 \cdot 3 \cdot 5 \cdot 3,607 \cdot 3,803 \\
1 & = \text{empty product}
\end{align*}
\]
If $n$ is composite, it has a factor of size at most $\sqrt{n}$.

$$n = p_1 \cdot p_2 \cdots p_k, \ k \geq 2$$

If $p_1 > \sqrt{n}, \ p_2 > \sqrt{n}$

$$\Rightarrow \ p_1 \cdot p_2 > n$$

$n \geq \sqrt{n}$

contradiction.
There are an infinite number of primes.

Proof by contradiction:
Suppose that there are only a finite number of primes:
\( p_1, p_2, \ldots, p_n \)

\[
\prod_{i=1}^{n} p_i + 1 = \prod_{i=1}^{n} p_i \equiv 0 \pmod{p_i}
\]

Contradiction.
• **Primality Testing**
  - Given an integer \( n \), determine if \( n \) is prime
  - Fermat’s little theorem test:
    
    If \( p \) is prime and \( a \neq 0 \), then \( a^{p-1} \equiv 1 \pmod{p} \)

• **Factoring**
  - Given an integer \( n \), determine the prime factorization of \( n \)
Factor the following 232 digit number [RSA768]:

123018668453011775513049495838496272077285
356959533479219732245215172640050726365751
874520219978646938995647494277406384592519
255732630345373154826850791702612214291346
167042921431160222124047927473779408066535
1419597459856902143413
GCD(a, b):

Largest integer \( d \) such that \( d \mid a \) and \( d \mid b \)

- \( \text{GCD}(100, 125) = 25 \)
- \( \text{GCD}(17, 49) = 1 \)
- \( \text{GCD}(11, 66) = 11 \)
- \( \text{GCD}(13, 0) = 13 \)
- \( \text{GCD}(180, 252) = 36 \)
GCD AND FACTORING

\[
a = 2^3 \cdot 3 \cdot 5^2 \cdot 7 \cdot 11 = 46,200
\]

\[
b = 2 \cdot 3^2 \cdot 5^3 \cdot 7 \cdot 13 = 204,750
\]

\[
\text{GCD}(a, b) = 2^{\min(3,1)} \cdot 3^{\min(1,2)} \cdot 5^{\min(2,3)} \cdot 7^{\min(1,1)} \cdot 11^{\min(1,0)} \cdot 13^{\min(0,1)}
\]

Factoring is expensive!
Can we compute \( \text{GCD}(a,b) \) without factoring?
If $a$ and $b$ are positive integers, then
\[ \gcd(a, b) = \gcd(b, a \mod b) \]

Proof:

By definition $a = (a \div b) \cdot b + (a \mod b) \pmod{d}$

If $d \mid a$ and $d \mid b$ then $d \mid (a \mod b)$.
If $d \mid b$ and $d \mid (a \mod b)$ then $d \mid a$. 
Repeatedly use the GCD fact to reduce numbers until you get $\text{GCD}(x, 0) = x$.

$\text{GCD}(660, 126) = \text{GCD}(126, 36)$
$= \text{GCD}(20, 6)$
$= \text{GCD}(6, 0)$
$= 6.$
GCD(x, y) = GCD(y, x mod y)

```c
int GCD(int a, int b){ /* a >= b, b > 0 */
    int tmp;
    while (b > 0) {
        tmp = a % b;
        a = b;
        b = tmp;
    }
    return a;
}
```

Example: GCD(660, 126)
If $a$ and $b$ are positive integers, then there exist integers $s$ and $t$ such that

$$\gcd(a,b) = sa + tb$$
**Extended Euclidean Algorithm**

\[ 13 \equiv 4 \pmod{35} \]

- Can use Euclid’s Algorithm to find \( s, t \) such that \( \gcd(a, b) = sa + tb \)

\[ \text{e.g. } \gcd(35, 27): \]

\[ 35 = 1 \cdot 27 + 8 \quad \text{35 - 1 \cdot 27 = 8} \]

\[ 27 = 3 \cdot 8 + 3 \quad \text{27 - 3 \cdot 8 = 3} \]

\[ 8 = 2 \cdot 3 + 2 \quad \text{8 - 2 \cdot 3 = 2} \]

\[ 3 = 1 \cdot 2 + 1 \quad \text{3 - 1 \cdot 2 = 1} \]

\[ 2 = 2 \cdot 1 + 0 \]

- Substitute back from the bottom

\[ 1 = 3 - 1 \cdot 2 = 3 - 1 \cdot (8 - 2 \cdot 3) = (-1) \cdot 8 + 3 \cdot 3 \]

\[ = (-1) \cdot 8 + 3 \cdot (27 - 3 \cdot 8) = 3 \cdot 27 + (-10) \cdot 8 \]

\[ \text{Valid in } \mathbb{Z}_{35} \]

\[ l \equiv 13 \cdot 27 \pmod{35} \]
Suppose \( \gcd(a, m) = 1 \)

By Bézout’s Theorem, there exist integers \( s \) and \( t \) such that \( sa + tm = 1 \).

\( s \mod m \) is the multiplicative inverse of \( a \):

\[
1 = (sa + tm) \mod m = sa \mod m
\]
Solving $ax \equiv b \pmod{m}$ for unknown $x$ when $\gcd(a, m) = 1$.

1. Find $s$ such that $sa + tm = 1$
2. Compute $a^{-1} = s \pmod{m}$, the multiplicative inverse of $a$ modulo $m$
3. Set $x = (a^{-1} \cdot b) \pmod{m}$
Solve: $7x \equiv 1 \pmod{26}$