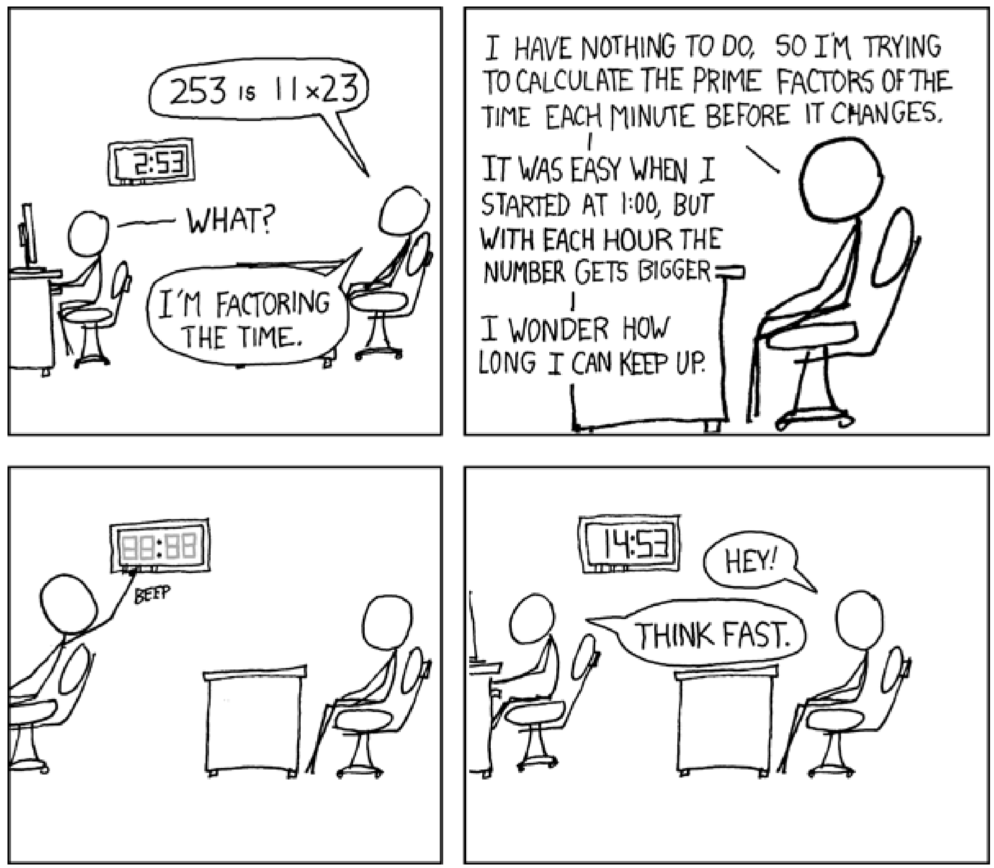
CSE 311: Foundations of Computing

Lecture 12: GCD and Solving Mod Equations



Last Class: +, $\times$ Properties of Mod

Let $\boldsymbol{m}$ be a positive integer. If $\boldsymbol{a} \equiv \boldsymbol{b} \pmod{\boldsymbol{m}}$ and $\boldsymbol{c} \equiv \boldsymbol{d} \pmod{\boldsymbol{m}}$, then

$$\boldsymbol{a} + \boldsymbol{c} \equiv \boldsymbol{b} + \boldsymbol{d} \pmod{\boldsymbol{m}}$$

$$\boldsymbol{ac} \equiv \boldsymbol{bd} \pmod{\boldsymbol{m}}$$

Last Class: Primality

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*.

Last Class: Fundamental Theorem of Arithmetic

Every positive integer greater than 1 has a unique prime factorization

$48 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3$
$591 = 3 \cdot 197$
$45{,}523 = 45{,}523$
$321{,}950 = 2 \cdot 5 \cdot 5 \cdot 47 \cdot 137$
$1{,}234{,}567{,}890 = 2 \cdot 3 \cdot 3 \cdot 5 \cdot 3{,}607 \cdot 3{,}803$

Last Class: Factoring is hard

Factor the following 232 digit number [RSA768]:

1230186684530117755130494958384962720772
8535695953347921973224521517264005072636
5751874520219978646938995647494277406384
5925192557326303453731548268507917026122
1429134616704292143116022212404792747377
94080665351419597459856902143413

12301866845301177551304949583849627207728535695953347
92197322452151726400507263657518745202199786469389956
47494277406384592519255732630345373154826850791702612
21429134616704292143116022212404792747377940806653514
19597459856902143413

$=$

334780716989568987860441698482126908177047949837
137685689124313889828837938780022876147116525317
43087737814467999489

$\times$

367460436667995904282446337996279526322791581643
430876426760322838157396665112792333734171433968
10270092798736308917

Last Class: Greatest Common Divisor

GCD(a, b):

Largest integer d such that $d \mid a$ and $d \mid b$

- GCD(100, 125) = 25
- GCD(17, 49) = 1
- GCD(11, 66) = 11
- GCD(13, 0) = 13
- GCD(180, 252) = 36 (= 2·2·3·3)

180=2·2·3·3·5   252=2·2·3·3·7

GCD and Factoring

$a = 2^3 \cdot 3 \cdot 5^2 \cdot 7 \cdot 11 = 46{,}200$

$b = 2 \cdot 3^2 \cdot 5^3 \cdot 7 \cdot 13 = 204{,}750$

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

Factoring is expensive!

Can we compute GCD(a,b) without factoring?

Useful GCD Fact

If a and b are positive integers, then

$$\gcd(a,b) = \gcd(b, a \bmod b)$$

Useful GCD Fact

If *a* and *b* are positive integers, then
gcd(*a*,*b*) = gcd(*b*, *a* mod *b*)

Proof:
By definition of mod, $a = qb + (a \bmod b)$ for some integer $q = a \operatorname{div} b$.

Let $d = \gcd(a, b)$. Then $d|a$ and $d|b$ so $a = kd$ and $b = jd$ for some integers k and j.

Therefore $(a \bmod b) = a - qb = kd - qjd = (k - qj)d$.
So, $d|(a \bmod b)$ and since $d|b$ we must have $d \leq \gcd(b, a \bmod b)$.

Now, let $e = \gcd(b, a \bmod b)$. Then $e|b$ and $e\,|(a \bmod b)$ so $b = me$ and $(a \bmod b) = ne$ for some integers m and n.

Therefore $a = qb + (a \bmod b) = qme + ne = (qm + n)e$.
So, $e|a$ and since $e|b$ we must have $e \leq \gcd(a, b)$.

It follows that $\gcd(a, b) = \gcd(b, a \bmod b)$. ∎

Another simple GCD fact

If a is a positive integer, $\gcd(a,0) = a$.

Euclid's Algorithm

gcd(a, b) = gcd(b, a mod b), gcd(a,0)=a

```
int gcd(int a, int b){ /* a >= b, b >= 0 */
    if (b == 0) {
        return a;
    }
    else {
        return gcd(b, a % b);
    }
```

Example: GCD(660, 126)

Euclid's Algorithm

Repeatedly use $\gcd(a, b) = \gcd(b, a \bmod b)$ to reduce numbers until you get $\gcd(g, 0) = g$.

gcd(660,126) =

Euclid's Algorithm

Repeatedly use $\gcd(a, b) = \gcd(b, a \bmod b)$ to reduce numbers until you get $\gcd(g, 0) = g$.

gcd(660,126) = gcd(126, 660 mod 126) = gcd(126, 30)
= gcd(30, 126 mod 30) = gcd(30, 6)
= gcd(6, 30 mod 6) = gcd(6, 0)
= 6

Euclid's Algorithm

Repeatedly use $\gcd(a, b) = \gcd(b, a \bmod b)$ to reduce numbers until you get $\gcd(g, 0) = g$.

$$
\begin{aligned}
\gcd(660,126) &= \gcd(126, 660 \bmod 126) = \gcd(126, 30) \\
&= \gcd(30, 126 \bmod 30) = \gcd(30, 6) \\
&= \gcd(6, 30 \bmod 6) = \gcd(6, 0) \\
&= 6
\end{aligned}
$$

In tableau form:

$$
\begin{aligned}
660 &= 5 * 126 + 30 \\
126 &= 4 * 30 + 6 \\
30 &= 5 * 6 + 0
\end{aligned}
$$

Bézout's theorem

If a and b are positive integers, then there exist integers $\boldsymbol{s}$ and $\boldsymbol{t}$ such that

$$\gcd(a,b) = \boldsymbol{s}a + \boldsymbol{t}b.$$

Extended Euclidean algorithm

- Can use Euclid's Algorithm to find s, t such that

$$\gcd(a, b) = sa + tb$$

Extended Euclidean algorithm

- Can use Euclid's Algorithm to find s, t such that

$$\gcd(a, b) = sa + tb$$

Step 1 (Compute GCD & Keep Tableau Information):

$$\gcd(\underset{a}{35}, \underset{b}{27}) = \gcd(\underset{b}{27}, \underbrace{\underset{a}{35} \bmod \underset{b}{27}}_{=r}) = \gcd(\underset{b}{27}, \underset{r}{8})$$

$$\underset{a}{35} = \underset{q}{1} * \underset{b}{27} + \underset{r}{8}$$

Extended Euclidean algorithm

- Can use Euclid's Algorithm to find s, t such that

$$\gcd(a, b) = sa + tb$$

Step 1 (Compute GCD & Keep Tableau Information):

$$\gcd(\underset{a}{35}, \underset{b}{27}) = \gcd(\underset{b}{27}, \underset{a \bmod b = r}{35 \bmod 27}) = \gcd(\underset{b}{27}, \underset{r}{8})$$

$$= \gcd(8, 27 \bmod 8) = \gcd(8, 3)$$

$$= \gcd(3, 8 \bmod 3) = \gcd(3, 2)$$

$$= \gcd(2, 3 \bmod 2) = \gcd(2, 1)$$

$$= \gcd(1, 2 \bmod 1) = \gcd(1, 0)$$

a	= q	* b	+ r
35	$= 1$	$* 27$	$+ 8$
27	$= 3$	$* 8$	$+ 3$
8	$= 2$	$* 3$	$+ 2$
3	$= 1$	$* 2$	$+ 1$

Extended Euclidean algorithm

- Can use Euclid's Algorithm to find s, t such that

$$\gcd(a, b) = sa + tb$$

Step 2 (Solve the equations for r):

a = q * b + r

$$35 = 1 * 27 + 8$$
$$27 = 3 * 8 + 3$$
$$8 = 2 * 3 + 2$$
$$3 = 1 * 2 + 1$$
$$2 = 2 * 1 + 0$$

r = a – q * b

$$8 = 35 - 1 * 27$$

Extended Euclidean algorithm

- Can use Euclid's Algorithm to find s, t such that

$$\gcd(a,b) = sa + tb$$

Step 2 (Solve the equations for r):

$a = q * b + r$	$r = a - q * b$
$35 = 1 * 27 + 8$	$8 = 35 - 1 * 27$
$27 = 3 * 8 + 3$	$3 = 27 - 3 * 8$
$8 = 2 * 3 + 2$	$2 = 8 - 2 * 3$
$3 = 1 * 2 + 1$	$1 = 3 - 1 * 2$
$2 = 2 * 1 + 0$	

Extended Euclidean algorithm

- Can use Euclid's Algorithm to find s, t such that

$$\gcd(a, b) = sa + tb$$

Step 3 (Backward Substitute Equations):

Plug in the def of 2

$$8 = 35 - 1 * 27$$

$$3 = 27 - 3 * 8$$

$$2 = 8 - 2 * 3$$

$$\boxed{1 = 3 - 1 * 2}$$

$$\begin{aligned} 1 &= 3 - 1 * (8 - 2 * 3) \\ &= 3 - 8 + 2 * 3 \\ &= (-1) * 8 + 3 * 3 \end{aligned}$$

Re-arrange into 3's and 8's

Extended Euclidean algorithm

- Can use Euclid's Algorithm to find s, t such that

$$\gcd(a, b) = sa + tb$$

Step 3 (Backward Substitute Equations):

$$8 = 35 - 1 * 27$$

$$3 = 27 - 3 * 8$$

$$2 = 8 - 2 * 3$$

$$\boxed{1 = 3 - 1 * 2}$$

Plug in the def of 2

$$\begin{aligned} 1 &= 3 - 1 * (8 - 2 * 3) \\ &= 3 - 8 + 2 * 3 \\ &= (-1) * 8 + 3 * 3 \end{aligned}$$

Re-arrange into 3's and 8's

Plug in the def of 3

$$\begin{aligned} &= (-1) * 8 + 3 * (27 - 3 * 8) \\ &= (-1) * 8 + 3 * 27 + (-9) * 8 \\ &= 3 * 27 + (-10) * 8 \end{aligned}$$

Re-arrange into 8's and 27's

$$\begin{aligned} &= 3 * 27 + (-10) * (35 - 1 * 27) \\ &= 3 * 27 + (-10) * 35 + 10 * 27 \\ &= 13 * 27 + (-10) * 35 \end{aligned}$$

Re-arrange into 27's and 35's

Multiplicative inverse $\mathrm{mod}\ m$

The *multiplication inverse mod* m *of* $a \bmod m$ is $b \bmod m$ iff $ab \equiv 1 \pmod{m}$.

x	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

mod 7

x	0	1	2	3	4	5	6	7	8	9
0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9
2	0	2	4	6	8	0	2	4	6	8
3	0	3	6	9	2	5	8	1	4	7
4	0	4	8	2	6	0	4	8	2	6
5	0	5	0	5	0	5	0	5	0	5
6	0	6	2	8	4	0	6	2	8	4
7	0	7	4	1	8	5	2	9	6	3
8	0	8	6	4	2	0	8	6	4	2
9	0	9	8	7	6	5	4	3	2	1

mod 10

Multiplicative inverse $\bmod m$

Suppose $\mathrm{GCD}(a, m) = 1$

By Bézout's Theorem, there exist integers s and t such that $sa + tm = 1$.

$s \bmod m$ is the multiplicative inverse of a:

$$1 = (sa + tm) \bmod m = sa \bmod m$$

Example

Solve: $7x \equiv 1 \pmod{26}$

Example

Solve: $7x \equiv 1 \pmod{26}$

$$\gcd(26,7) = \gcd(7,5) = \gcd(5,2) = \gcd(2,1) = 1$$

$$\begin{aligned} 26 &= 7 * 3 + 5 & \quad 5 &= 26 - 7 * 3 \\ 7 &= 5 * 1 + 2 & 2 &= 7 - 5 * 1 \\ 5 &= 2 * 2 + 1 & 1 &= 5 - 2 * 2 \end{aligned}$$

$$\begin{aligned} 1 &= 5 - 2 * (7 - 5 * 1) \\ &= (-7) * 2 + 3 * 5 \\ &= (-7) * 2 + 3 * (26 - 7 * 3) \\ &= (-11) * 7 + 3 * 26 \end{aligned}$$

Multiplicative inverse of 7 mod 26

Now $(-11) \bmod 26 = 15$. **So,** $x = 15 + 26k$ **for** $k \in \mathbb{Z}$.

Example of a more general equation

Now solve: $7y \equiv 3 \pmod{26}$

We already computed that 15 is the multiplicative inverse of 7 modulo 26:

That is, $7 \cdot 15 \equiv 1 \pmod{26}$

By the multiplicative property of mod we have

$$7 \cdot 15 \cdot 3 \equiv 3 \pmod{26}$$

So any $y \equiv 15 \cdot 3 \pmod{26}$ is a solution.

That is, $y = 19 + 26k$ for any integer k is a solution (since $45 \bmod 26 = 19$. We could also leave as 45.)

Math mod a prime is especially nice

$\gcd(a, m) = 1$ **if** m **is prime and** $0 < a < m$ **so can always solve these equations mod a prime.**

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

X	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

mod 7

Modular Exponentiation mod 7

x	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

a	a^1	a^2	a^3	a^4	a^5	a^6
1						
2						
3						
4						
5						
6						

Repeated Squaring – small and fast

Since $a \bmod m \equiv a \pmod{m}$ and $b \bmod m \equiv b \pmod{m}$

we have $ab \bmod m = ((a \bmod m)(b \bmod m)) \bmod m$

So $\quad a^2 \bmod m = (a \bmod m)^2 \bmod m$

and $\quad a^4 \bmod m = (a^2 \bmod m)^2 \bmod m$

and $\quad a^8 \bmod m = (a^4 \bmod m)^2 \bmod m$

and $\quad a^{16} \bmod m = (a^8 \bmod m)^2 \bmod m$

and $\quad a^{32} \bmod m = (a^{16} \bmod m)^2 \bmod m$

Can compute $a^{2^i} \bmod m$ in only i steps

What if exponent is not a power of 2?

Fast Exponentiation Algorithm

81453 in binary is 10011111000101101

$$81453 = 2^{16} + 2^{13} + 2^{12} + 2^{11} + 2^{10} + 2^{9} + 2^{5} + 2^{3} + 2^{2} + 2^{0}$$

$$a^{81453} = a^{2^{16}} \cdot a^{2^{13}} \cdot a^{2^{12}} \cdot a^{2^{11}} \cdot a^{2^{10}} \cdot a^{2^{9}} \cdot a^{2^{5}} \cdot a^{2^{3}} \cdot a^{2^{2}} \cdot a^{2^{0}}$$

$$\begin{aligned}
&a^{81453} \bmod m = \\
&(\ldots(((((a^{2^{16}} \bmod m \cdot \\
&\quad a^{2^{13}} \bmod m\ ) \bmod m \cdot \\
&\quad\; a^{2^{12}} \bmod m) \bmod m \cdot \\
&\quad\;\; a^{2^{11}} \bmod m) \bmod m \cdot \\
&\quad\;\;\; a^{2^{10}} \bmod m) \bmod m \cdot \\
&\quad\;\;\;\; a^{2^{9}} \bmod m) \bmod m \cdot \\
&\quad\;\;\;\;\; a^{2^{5}} \bmod m) \bmod m \cdot \\
&\quad\;\;\;\;\;\; a^{2^{3}} \bmod m) \bmod m \cdot \\
&\quad\;\;\;\;\;\;\; a^{2^{2}} \bmod m) \bmod m \cdot \\
&\quad\;\;\;\;\;\;\;\; a^{2^{0}} \bmod m)\ \ \bmod m
\end{aligned}$$

The fast exponentiation algorithm computes $a^k \bmod m$ using $\leq 2\log k$ multiplications $\bmod m$

Using Fast Modular Exponentiation

- Your e-commerce web transactions use SSL (Secure Socket Layer) based on RSA encryption
- RSA
  - Vendor chooses random 512-bit or 1024-bit primes p, q and 512/1024-bit exponent e. Computes $m = p \cdot q$
  - Vendor broadcasts (m, e)
  - To send a to vendor, you compute $C = a^e \bmod m$ using *fast modular exponentiation* and send C to the vendor.
  - Using secret p, q the vendor computes d that is the *multiplicative inverse* of e mod $(p-1)(q-1)$.
  - Vendor computes $C^d \bmod m$ using *fast modular exponentiation*.
  - Fact: $a = C^d \bmod m$ for $0 < a < m$ unless $p|a$ or $q|a$