Primes:

$$90 = 2 \cdot 45 = 2 \cdot 9 \cdot 5 = 2 \cdot 3^2 \cdot 5$$

$$375 = 3 \cdot 5^3$$

47 is prime? $\sqrt{47} \approx 6. \dots\dots$

Check does 2, 3, 4, 5, 6 divide 47

$$2145 = 715 \cdot 3 = 143 \cdot 5 \cdot 3 = 11 \cdot 13 \cdot 5 \cdot 3 = 3 \cdot 5 \cdot 11 \cdot 13$$

GCD:

$$\left.\begin{array}{l} \text{If } b \text{ divides } a \\ \quad \text{return } b \\ \text{else return}(\gcd(b, a \bmod b)) \end{array}\right\} \text{Recursive Algorithm}$$

ex:

$\gcd(52, 44) = 4$

$\underline{s} \cdot 52 + \underline{t} \cdot 44 = 4$

$\gcd(391, 62)$

$391 = 6 \cdot 62 + 19$

$62 = 3 \cdot 19 + 5$

$19 = 3 \cdot 5 + 4$

$5 = 1 \cdot 4 + 1$

$4 = 1 \cdot 4 + 0$

$\gcd(\overset{a}{391}, \overset{b}{62})$

$\downarrow$

$\gcd(\overset{a}{62}, \overset{b}{19})$

$\gcd(\overset{a}{19}, \overset{b}{5})$

$\gcd(\overset{a}{5}, \overset{b}{4})$

$\gcd(\overset{a}{4}, \overset{b}{1})$

$\gcd(621, 483)$

$621 = 1 \cdot 483 + 138$

$483 = 3 \cdot 138 + 69$

Solving Congruences:

Case 1:

$$a + x \equiv b \mod n$$

$$x \equiv b - a \mod n$$

ex:

$$3 + x \equiv 10 \mod 4$$

$$x \equiv 7 \mod 4$$

$$x \equiv 3 \mod 4$$

← smallest positive solution

Case 2:

$$-a + x \equiv b \mod n$$

$$x \equiv b + a \mod n$$

ex:

$$-3 + x \equiv 9 \mod 4$$

$$x \equiv 12 \mod 4$$

$$x \equiv 0 \mod 4$$

Case 3:

$$a \cdot x \equiv b \mod n$$

In an ideal world:

$$\frac{1}{a} \cdot a \cdot x \equiv \frac{1}{a} \cdot b \mod n$$

but $\frac{1}{a}$ is not defined!

Let $c = a^{-1}$, i.e. c is the inverse of a

$$7x = 14$$

$$\frac{1}{7} \cdot 7 \cdot x = \frac{1}{7} \cdot 14$$

$$x = 2$$

Multiplicative inverse:

y is an inverse of x mod n iff.

$$x \cdot y \equiv 1 \mod n$$

Case 3 (revisited):

$$a x \equiv b \mod n$$

$$c \cdot a \cdot x \equiv b \cdot c \mod n \qquad \text{where } c = a^{-1}$$

$$a^{-1} \cdot a \cdot x \equiv b \cdot a^{-1} \mod n$$

$$x \equiv b \cdot a^{-1} \mod n$$

$$\frac{1}{7} \cdot 7x = 14 \cdot \frac{1}{7}$$

<u>ex:</u>

$$5 \cdot x \equiv 6 \mod 7$$

Which number leaves a remainder of 1 when multiplied to 5 mod 7?

$$5 \cdot a^{-1} \mod 7 \equiv 1$$

$$5 \cdot 1 \mod 7 \equiv 5$$

$$5 \cdot 2 \mod 7 \equiv 3$$

$$5 \cdot 3 \mod 7 \equiv 1 \leftarrow \text{yes!}$$

$$\underbrace{3 \cdot 5}_{} \cdot x \equiv 3 \cdot 6 \mod 7$$

$$x = 4$$

ex:

$3x \equiv 2 \mod 8$

$3 \cdot 3x \equiv 3 \cdot 2 \mod 8$

$x = 6$

ex:

$2x \equiv 4 \mod 6$

2 and 6 are not coprime: $\gcd(6,2) \neq 1$

so $\gcd(a,n) = 1$

ex:

$15x \equiv 7 \mod 26$

How to find Inverse:

1) Guess
2) Extended Euclidean Algorithm (EEA)
3) Euler's Theorem*

Euler's Theorem:

If $\gcd(a,n)=1$ and $n \geq 2$

$$a^{\Phi(n)} \equiv 1 \mod n$$

$7^4 \equiv$ ~

It follows that:

$7 \cdot 7^{4-1} \equiv$ ~

$$a \cdot \underbrace{a^{\Phi(n)-1}}_{\text{This is invers of } a \bmod n} \equiv 1 \mod n$$

$a^{\Phi(n)-1}$ is inverse of $a \bmod n$

Euler's phi Function:

The number of integers in $\mathbb{Z}_m$ relatively Prime to m is denoted $\phi(m)$:

$$39 = 3 \cdot 13$$

$$(p-1)\cdot(q-1)$$

$$\phi(m) = \prod_{i=1}^{t} \left(p_i^{a_i} - p_i^{a_i - 1}\right)$$

__Ex:__ $m = 240$

$$= 2 \cdot 120 = 2 \cdot 2 \cdot 60 = 2 \cdot 2 \cdot 2 \cdot 30 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 15$$

$$= 2^4 \cdot 3 \cdot 5$$

$$\phi(m) = (2^4 - 2^3) \cdot (3^1 - 3^0)(5^1 - 5^0) = 8 \cdot 2 \cdot 4 = \underline{\underline{64}}$$

$$a^{\phi(n)} \equiv 1 \mod m$$

What if n is prime?

$$a^{p-1} \equiv 1 \mod p$$ Fermat's Little Theorem.

$$a \cdot a^{p-2} \equiv 1 \mod p$$

This is inverse.

Ex:

$2x \equiv 5 \mod 7$

$a^{-1} = 2^{7-2} = 2^5 = 32 \mod 7 \equiv 4$

$x = 5 \cdot 4 \mod 7 \to x = 6$

ex:

$2 \cdot 13$

$15x \equiv 7 \mod 26$

$15^{\phi(26)-1} \mod 26 \to 15^{11} \mod 26$

$15^2 \cdot 15^2 \cdot 15^2 \cdot 15^2 \cdot 15^2 \cdot 15 \mod 26$

$17 \cdot 17 \cdot 17 \cdot 17 \cdot 17 \cdot 15$

Fast Exponentiation:

naive

$x^{2^{1024}}$

$x \cdot x = x^2$

$x^2 \cdot x = x^3$

$x^3 \cdot x = x^4$

$\vdots$

$x^{2^{1024}-1} \cdot x = x^{1024}$

mult

$2^{1024} - 1$

linear

Better

$x^{2^{1024}}$

$x \cdot x = x^2$

$x^2 \cdot x^2 = x^4$

$x^4 \cdot x^4 = x^8$

3 mult

2^3

1024 mult

logarithmic

Square and Multiply:

ex : $3^{400} \bmod 11$?

1. Find binary representation of exponent

   $400_{10} \rightarrow 256+128+16 = 110010000$

2. Scan bits from left to right

   a) If 1 square and multiply

   b) If 0 square

1	$3 \bmod 11$	
1	$3^2 \cdot 3 \bmod 11$	$= 5$
0	$5^2 \bmod 11$	$= 3$
0	$3^2 \bmod 11$	$= 9$
1	$9^2 \cdot 3 \bmod 11$	$= 1$
0	1^2	$= 1$
0		$= 1$
0		$= 1$
0		$= 1$

$17^{42} \equiv 1 \mod 43$

So 17^{41} is inverse

1. $41 \to 101001$

1	$17 \mod 43$	$=$	17
0	$17^2 \mod 43$	$=$	31
1	$31^2 \cdot 17$	$=$	40
0	40^2	$=$	9
0	9^2	$=$	~~38~~
1	$38^2 \cdot 17$	$=$	38

Using this for even cooler stuff:

$7^{222} \mod 11$, $\Phi(p) = p-1 \rightarrow 7^{10} = 1 \mod 11$

$7^{10 \cdot 22 + 2} \mod 11$

$(7^{10})^{22} \cdot 7^2 \mod 11 = \underline{\underline{5}}$

$7^{256} \mod 13$

$\underset{10}{7}^{12 \cdot 21} \cdot \underset{10}{7}^{4} \mod 13$

$(7 \cdot 7)(7 \cdot 7) \mod 13 = \underline{\underline{9}}$

$2^{245} \mod 11 \rightarrow \Phi(n) = 10$

$2^{10 \cdot 24 + 5} = (2^{10})^{24} \cdot 2^5 \mod 11$

$= \underline{\underline{10}}$

$\Phi(n) = 10$

$3^{400} \mod 11$

The RSA Algorithm:

2048 bits

1. Find large primes p, q

2. $n = p \cdot q$, $\Phi(n) = (p-1) \cdot (q-1)$

3. Choose a value e (public key) s.t.

$$\gcd(e, \Phi(n)) = 1$$

4. find Inverse of $e \bmod \Phi(n)$, i.e.

$$e \cdot \underline{d} \equiv 1 \mod \Phi(n)$$

e, d, n

Encryption:

$m^e \mod n = c$ Ciphertext Ciphervalue

Decrypt:

$c^d \mod n = m$

$$c^d = (m^e)^d$$
$$= m^{e \cdot d}$$
$$= m^1$$