Solving the Single linear Congruence

$ax \equiv c \pmod m$, $d = \gcd(a, m)$, $d \mid c$. —— (1)

1. No soln if $d \nmid c$
2. Solve the modified congruence

$$\frac{a}{d} y \equiv \frac{c}{d} \pmod{\frac{m}{d}} \quad \text{—— (2)}$$

which has a unique soln: y_0 as $\gcd\left(\frac{a}{d}, \frac{m}{d}\right) = 1$.

3. The d solns of the original congruence are

$y_0 + i\frac{m}{d}$, $0 \le i \le d-1$.

$\pmod m$

Proof of Correctness

Claim 1 d solns indicated by the algm. actually solve the original congruence (1)

proof. $\frac{a}{d} y_0 \equiv \frac{c}{d} \pmod{\frac{m}{d}}$

$\Rightarrow \frac{m}{d} \mid \left[\frac{a}{d} y_0 - \frac{c}{d}\right]$

$\Rightarrow m \mid (ay_0 - c) \Rightarrow ay_0 \equiv c \pmod m$

$\Rightarrow y_0$ is a soln.

$d = \gcd(a, m) \Rightarrow d \mid a$

$\frac{a}{d}\left(y_0 + \frac{im}{d}\right)$

$\equiv \frac{a}{d} y_0 + \frac{aim}{d}$

$\equiv c \pmod m$

$\Rightarrow y_0 + \frac{im}{d}$ is a soln

$1 \le i \le d-1$

Claim There are no other soln^s $\pmod m$.

proof:

Note No other soln^s of (1) of the form

$$y_0 + \frac{im}{d} \pmod m,$$

$i \in \mathbb{Z}$;

other than d soln^s indicated by the alg^m

Because for any integer $i \in \mathbb{Z}$, if $r = i \bmod d$,

then $y_0 + \frac{im}{d} \equiv y_0 + \frac{rm}{d} \pmod m$

To prove (1) has no soln^n other than these.

Suppose z_0 is a soln^n of (1)

$\therefore az_0 \equiv c \pmod m$ — (2).

$\therefore \exists$ unique int. i s.t.

$$y_0 + \frac{im}{d} \leq z_0 < y_0 + \frac{(i+1)m}{d}$$

$$\Rightarrow \frac{im}{d} \leq z_0 - y_0 < \frac{(i+1)m}{d}.$$

$$\Rightarrow z_0 \not\equiv y_0 \pmod m$$

(2)

$\Rightarrow \frac{a}{d} z_0 \equiv \frac{c}{d} \pmod{\frac{m}{d}}$ which contradicts the fact that y_0 is the unique soln^n of this congruence (2).

Chinese Remainder Theorem

① $\begin{cases} x \equiv a_1 \pmod{n_1} \\ x \equiv a_2 \pmod{n_2} \\ \vdots \\ x \equiv a_k \pmod{n_k} \end{cases}$

$n_1, n_2, \cdots, n_k$ pairwise relatively prime

↳ unique sol^n.

$$x \equiv \sum_{i=1}^{k} a_i N_i M_i \pmod{n} \quad \text{—— ②}$$

$a_i N_i (N_i^{-1} \bmod n_i) \pmod{n}$

↓

$N_i = \frac{n}{n_i}$

where $n = n_1 n_2 \cdots n_k$

$N_i = \frac{n}{n_i}$

$M_i = N_i^{-1} \bmod n_i$

proof. (Existence)

$\gcd(N_i, n_i) = 1, \quad 1 \le i \le k.$

$\therefore \exists$ unique sol^n M_i of the congruence

$$N_i M_i \equiv 1 \pmod{n_i}.$$

Claim: $x = \sum_{i=1}^{k} a_i N_i M_i$ is a simultaneous sol^n. of eqn. ②:

Now ~~$N_i \bmod n_j$~~ $N_i \equiv 0 \pmod{n_j}$ unless $i = j$

$\therefore x = a_1 N_1 M_1 + a_2 N_2 M_2 + \cdots + a_j N_j M_j + \cdots + a_k N_k M_k$

$\equiv \cancel{0 + 0 + \cdots + a_j N_j M_j} \pmod{n_j}$

$\equiv a_j N_j M_j \pmod{n_j} \equiv a_j \cdot 1 \equiv a_j \pmod{n_j}$

Uniqueness

x' → another simultaneous soln. of equn. (1).

$\therefore \forall i,\ 1 \le i \le k$, $\quad x \equiv a_i \equiv x' \pmod{n_i}$.

$\Rightarrow \quad n_i \mid x - x'$

Since the n_i's are pairwise relatively prime, their product

$n = n_1 n_2 \cdots n_k$ also divides $x - x'$

i.e. $\quad n \mid x - x'$

i.e. $\quad x \equiv x' \pmod{n}$.

An application of factoring : Remote Coin Flipping

- Suppose that two people, Alice & Bob, wish to flip coin while they are conversing over a public channel.
- Each entertain a doubt :
  Could the person flipping the coin possibly cheat, by telling the party who calls the outcome that they are wrong — no matter how the coin turns up?
- Without relying on trusted witness, can a procedure be set up that cannot be biased by either Alice or Bob?
- In 1982, Manuel Blum devised a number-theoretic scheme, a two party protocol, which meets the specifications of a coin toss : that is, the probability of correctly guessing the outcome is 1/2.
- The game's security against duplicity hinges on the difficulty of factoring integers that are product of two large primes of roughly the same size.

Note. $x^2 \equiv a \pmod n$, $n = pq$, p, q prime.

Square root of $a \bmod n$

4 square roots mod n obtained by

Solving $x^2 \equiv a \pmod p \rightarrow$ two Square roots mod p $(\pm x_1)$

$x^2 \equiv a \pmod q \rightarrow$ two square roots mod q $(\pm x_2)$

Use CRT $x = \pm x_1 \bmod p$, $x = \pm x_2 \bmod q$ $\rightarrow$ four sol^n $x \bmod pq$.

- p, q both $4k+3$ type.

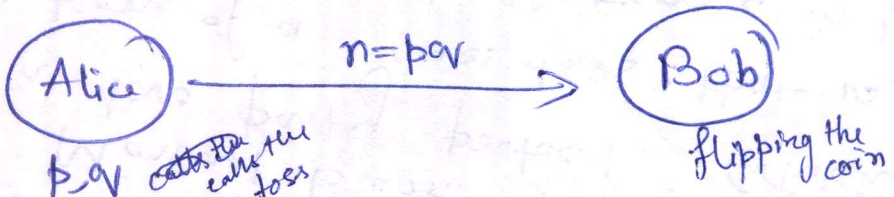
→ $x^2 \equiv a \pmod p$ has two sol^{ns}. $x_1 = \pm a^{\frac{p+1}{4}} \bmod p$

→ $x^2 \equiv a \pmod q$ has two sol^{ns}. $x_2 = \pm a^{\frac{q+1}{4}} \bmod q$.

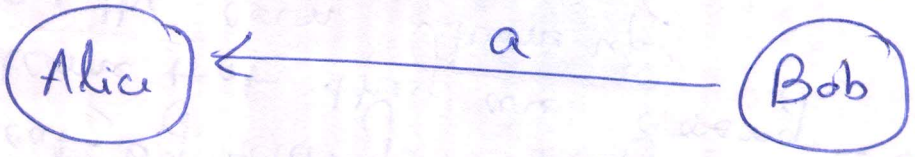
Then use CRT to get 4 square roots mod n

Blum's protocol

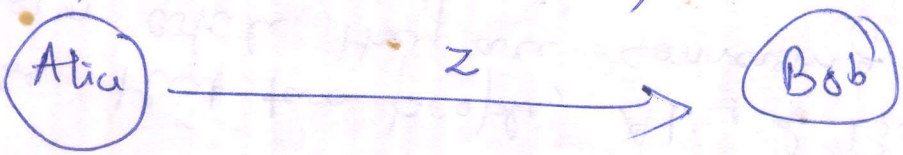
1. Alice begins by chosing two large primes p and q, both congruent to 3 modulo 4. She announces only their product $n = pq$ to Bob.



2. Bob responds by ~~responds by~~ randomly selecting an integer x, $0 < x < n$ with $\gcd(x, n) = 1$. He sends its square, $a \equiv x^2 \pmod n$, to Alice. (This corresponds to the coin flipping).



3. Knowing p, q, Alice calculates $a = x^2 \bmod n$ the four square roots $x, -x, y, -y$ of a modulo n. She picks one of them to send to Bob.
(That is, Alice calls the toss)



$z \in_R \{x, -x, y, -y\}$

4. If Bob receives x or $-x$, he declares Alice to have guessed correctly. Otherwise, Bob wins; for he ~~will be~~ is able to factor n.

??

(A winner announced)

Alice ← b, π for b — Bob

b ∈ { Alice wins, Alice fails } prod π

Note

- each of the parties knows a different secret during the course of the game.
  - p, q are Alice's concealed information.
  - x is Bob's ~~secret~~ personal secret
- Alice has no way of knowing x, so her guess at ±x among the possible square roots of a is a real one, with a 50% chance of success.
  i.e. Pr (z = ±x) = 1/2.
- If Bob receives y or −y from Alice, then he possesses two different square roots of a mod n.

He will be able to convince Alice that she has guessed incorrectly by sending back to her the factors p and q of n.

how?

He simply calculates gcd (x ± y, n).

As $x^2 \equiv a \equiv y^2 \pmod n$; $x \not\equiv \pm y \pmod n$, we get-

$n \mid (x^2 - y^2)$ but $n \nmid (x+y)$ & $n \nmid (x-y)$

$pq \mid (x+y)(x-y)$ (*)

As (p, q) = 1, if both p, q divide (x+y), then n is a factor of x+y & so a factor of x−y. (→←)

⇒ each prime divides either x+y or x−y, although both cannot divide the factor.

∴ gcd (x+y, n) is either p or q and gcd (x−y, n) produces the other factor.

If both p, q divide x+y, then we get a contradiction to (*)

x^2

- On the other hand, if Bob receives either x or $-x$, then he has learnt nothing new & is unable to factor n in a reasonable length of time. His failure to do so is an admission that Alice has won the game.

After the game is over, she can assure Bob that she used a Blum integer n by providing its factors p, q. Bob should check that the disclosed factors are indeed primes

Toy Example: (for real application, primes should be large, 100 or more digits).

$p = 43$, $q = 71$

$43 = 4 \times 10 + 3$
$71 = 4 \times 17 + 3$

1. Alice publishes $n = 3053 = 43 \times 71$
2. Bob computes, chooses $x = 192$, $0 < x < n$
   $\gcd(x, n) = 1$.

   Computes $a = x^2 \bmod 3053$
   $= 228 \bmod 3053$

   sends 228.

3. Alice computes 4 square roots of 228 mod 3053:

$x^2 = 228 \bmod 43$, $x^2 = 228 \bmod 71$
$= 13 \bmod 43$, $= 15 \bmod 71$

gives $x = \pm (13)^{\frac{43+1}{4}} \bmod 43$, $x = \pm (15)^{\frac{71+1}{4}} \bmod 71$

$= \pm 20 \bmod 43$ $= \pm 24 \bmod 71$

CRT $x = 192, 2861, 1399, 1654 \bmod 3053$

192, 2861 → Bob's secret no. x

1399, 1654 → not Bob's secret no. x.

Alice has an even chance of picking a "correct" number.

- Suppose that Alice makes a nonwinning choice by guessing at 1399.
  i.e. Bob has won the toss.
  But Alice prudently challenges Bob to prove it.

So Bob determines the factorization of 3053 by calculating:

gcd (1591, 3053) = gcd (1399 + 192, 3053) = 43.

(Extended Euclidean algm)

gcd (−1207, 3053) = gcd (1399 − 192, 3053) = 71.

He sends these factors to Alice to confirm that she has chosen incorrectly.

- If Alice makes a winning choice by guessing at 192.
  i.e. Bob has lost the toss, he will not be able to ~~guarantee~~ factors of n in reasonable time bound.
  Alice can convince Bob that she used a Blum integer by providing its factors.
  Bob can check the disclosed factors are indeed primes.

Monte carlo randomized algm. for primality testing

→ $O((\log n)^2)$.

→ output correct with high probability.

→ if the input is prime, it never gives incorrect answer.

→ However, if the input is composite, then the answer may be incorrect with small prob.

(one-sided error).

e.g. fermat's primality test.

if x is prime, then $x^{n-1} \equiv 1 \pmod n$ for $x < n$

↓ use contrapositive statement

↓ sufficiently large to ensure a prob. of correctness of $1 - 1/n^{\alpha}$

fails for Carmichael nos. 561, 1105.

```
FPrime (n, α)
// α is prob. parameter
q := n-1;
for i := 1 to range do // Specify large
                       // range = 100
    m := q; y := 1;
    x := Random( ) mod q + 1;
    // choose a random no. in the
    // range [0, n-1]
    // x is called witness
    z := x;
    // Compute x^(n-1) mod n
    while (m > 0) do
        while (m mod 2 = 0) do
            z := z^2 mod n;
            m := ⌊m/2⌋;
        end do
        m := m-1; y := (y * z) mod n;
    end do
    if (y ≠ 1) then
        return false;
        // x^(n-1) mod n ≠ 1 ⇒ n not prime & x is the witness for this
    end do
    return true
    // n is probably prime
end prime.
```

Carmichael no. means

every $x < n$ with $\gcd(x,n) = 1$ ~~satisfy~~ Satisfies fermat's eqn.

∴ witness x for compositeness of n can be determined only if x happens to be a factor of n.

Miller-Rabin primality test

> if n is prime, then $x^2 \equiv 1 \pmod n$ has exactly two s.f.s, namely 1 & $n-1$.

$a^{n-1} \equiv 1 \bmod n$

$a^{\frac{n-1}{2}} = \pm 1 \bmod n$

$\tilde{x} \to x, x^2, x^3, \ldots$

$z \to x^2, x^4, x^6, \ldots$

```
MRPrime(n, α)
    v := n-1;
    for i := 1 to α x log n do
        m := v ; y := 1;
        x := Random() mod v + 1;
        z := x ; // Compute x^(n-1) mod n
        while (m > 0) do
            while (m mod 2 = 0) do
                x̃ := z ;  z := z^2 mod n ;
                if ((z = 1) ∧ (x̃ ≠ 1) ∧ (x̃ ≠ v)) then
                    return false ; // x̃ is a non trivial sq. root of 1, so n is not prime & x is the witness for this
                end if
                m := ⌊m/2⌋ ;
            end do
            m := m-1 ; y := (y * z) mod n ;
        end do
    if (y ≠ 1) return false
        // x^(n-1) mod n ≠ 1 & n is not prime & x is a witness for this
    end do
    return true ; probably prime.
```

Miller-Rabin Test

Proposition Suppose p is an odd prime & $1 < a < p-1$

& $p-1 = 2^f \cdot m$, m is odd

Then either $a^m \equiv 1 \pmod p$ or $a^{2^j m} \equiv -1 \pmod p$

for some j, $0 \le j < f$.

Contrapositive

If $n > 1$ odd with $n-1 = 2^f \cdot m$, m odd, we can find an integer a, with $1 < a < n-1$ s.t.

$a^m \not\equiv 1 \pmod n$ and $a^{2^j m} \not\equiv -1 \pmod n$

$\forall\ j$, $0 \le j < f$, then n is Composite.

- $n-1 = 2^f \cdot m$, m odd
- chose a, $1 \le a \le n-1$
- $b \leftarrow a^m \pmod n$

if $b \equiv 1 \pmod n$ if count = k

count = count + 1 "n is probably prime"

return

else

for $i := 0$ to $f-1$ do

if $b \equiv -1 \pmod n$ if count = k then

count = count + 1 "n is probably prime"

return

else

$b \leftarrow b^2 \bmod n \rightarrow a^{2m}, a^{2^2 m}, \ldots, a^{2^{f-1} m}$

end do

return "n is Composite with witness a"

k iterations

error prob. $< \left(\frac{1}{4}\right)^k$

e.g. $k = 20$

$\left(\frac{1}{4}\right)^{20} \approx 9.0949 \times 10^{-13}$

< 1 in 1 trillion

Ans. Composite → result is correct

Ans. probably prime → result incorrect with prob. $\left(\frac{1}{4}\right)^k$

$O(\log^3 n)$

Euler's Criterion

- if p is odd prim

then $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p$

$\left(\frac{a}{p}\right)$ Legendre Symbol if p prim

↳ ± 1

when $p \nmid a$

0 when $p \mid a$

Contraposition

n odd int., $1 \le a \le n-1$

if $\left(\frac{a}{n}\right) \not\equiv a^{\frac{n-1}{2}} \pmod n$ then n is composite.

$\left(\frac{a}{n}\right)$ Jacobi Symbol. if n composite

- Choose a, $1 \le a \le n-1$
- Compute $\left(\frac{a}{n}\right)$ (Jacobi Symbol)
- Compute $a^{\frac{n-1}{2}} \pmod n$

if $\left(\frac{a}{n}\right) \not\equiv a^{\frac{n-1}{2}} \pmod n$

return "n is composite"

else Count = count + 1; if count $= k$ then return "n is probably prim"

after k iteration else.

error prob → can not be reduced much by increasing iteration k

complexity → $O((\log n)^3)$

Solovay - Strassen

$1 \leq a \leq n-1$

if $\left(\frac{a}{n}\right) \not\equiv a^{\frac{n-1}{2}} \pmod n$

then n is composite & a is a witness.

Let

$A \rightarrow$ a random odd integer n of a ~~specific~~ size is composite.

$B \rightarrow$ the algm answers 'n is probably prime' after ~~k~~ iterations

$$Pr(B|A) < 2^{-k} \qquad Pr(B|\bar{A}) = 1$$

$$Pr(A|B) = ?$$

↳ error probability.

Let $N < n < 2N$

By prime no. theorem, the # of odd primes between N & $2N$ is approximately

$$\frac{2N}{\ln 2N} - \frac{N}{\ln N} \approx \frac{N}{\ln N} \approx \frac{n}{\ln n}$$

∴ There are $\frac{N}{2} \approx \frac{n}{2}$ odd integers between N & $2N$, we can use the estimate $Pr(A) \approx 1 - \frac{2}{\ln n}$

$$\therefore Pr(A|B) = \frac{Pr(B|A)\,Pr(A)}{Pr(B|A)\,Pr(A) + Pr[B|\bar{A}]\,Pr[\bar{A}]}$$

$$\approx \frac{Pr(B|A) \cdot [1 - 2/\ln n]}{Pr[B|A]\left(1 - \frac{2}{\ln n}\right) + \frac{2}{\ln n}}$$

$$1 - \frac{n/\ln n}{n/2}$$

$$= \frac{Pr(B|A)(\ln n - 2)}{Pr(B|A)(\ln n - 2) + 2}$$

$$\leq \frac{2^{-k}(\ln n - 2)}{2^{-k}(\ln n - 2) + 2}$$

$$= \frac{\ln n - 2}{\ln n - 2 + 2^{k+1}}$$

$\bar{A}$ → a random odd integer n is prime.

k	Error prob.
10	$\cdot 168 \times 10^{-3}$
20	$\cdot 169 \times 10^{-6}$
30	$\cdot 157 \times 10^{-12}$
50	$\cdot 139 \times 10^{-27}$
100	

prob. of error is reduced to a very small amount with the increase in the no. of iterations

AKS primality Test

Deterministic - $O(\log^{13} n)$

↓ improved to $O(\log^{6} n)$

SS / MR → $O(\log^{3} n)$