P THINK FAST S

Competitive Programming

From Problem 2 Solution in O(1)

Number Theory

Diophantine Equation and Congruence

Mostafa Saad Ibrahim
PhD Student @ Simon Fraser University

Diophantine equation

- A **Diophantine equation** is an equation in which only **integer solutions** are allowed.
- It has as either **no** solutions ($x^2 + 4y = 3$), or **infinitely** many solutions ($x + y = 1$)
- $ax + by = c$ is a **linear** Diophantine equation in two variables (x, y)
- $x^2 + y^2 = z^2$ is a **nonlinear second-degree** Diophantine equation of 3 variables (Pythagorean triple)

Linear Diophantine equation

- We will focus on: ax + by = c
  - Degenerate case (a, b, c are 0) => infinite solutions
- This equation has solution IFF c % gcd(a, b) = 0. Please read proof on wiki.
- If we assumed c = g = gcd(a, b)
  - ax + by = gcd(a, b) => we solved that by **extended** algo
- Or generally, if c % g = 0, Let t = c /g
  - multiply all equation with t
  - axt + byt = g * t = c   (xt, yt) is one solution
  - In other words, solve extended and multiply by c/g

Linear Diophantine equation

- 258x+147y = 369
  - gcd(258, 147) = 3 and 3 divides 369? Yes!
  - Solve by extended: 258x+147y = 3
  - 258(4)+147(−7) = 3 (multiply by 123 = 369/3)
  - 258(492)+147(−861)=369 => ONE solution
- All solutions: Bézout's identity
  - x = 492 − 147r / 3 = 492−49r
  - y =−861 + 258r / 3 = 86r−861

$$\begin{cases} x = x_0 + k \cdot b/g, \\ y = y_0 - k \cdot a/g, \end{cases} \quad k \in Z$$

- You can reduce constants by r = t+10
  - x = 492 − 49(t+10) = 2−49t
  - y = 86(t+10) − 861=86t−1

Linear Diophantine equation: code

```
ll extended_euclid(ll a, ll b, ll &x, ll &y) {
    if (a < 0) {
        ll r = extended_euclid(-a, b, x, y);
        x *= -1;
        return r;
    }
    if (b < 0) {
        ll r = extended_euclid(a, -b, x, y);
        y *= -1;
        return r;
    }
    if (b == 0) {
        x = 1;
        y = 0;
        return a;
    }
    ll g = extended_euclid(b, a % b, y, x);
    y -= (a / b) * x;
    return g;
}

// Find any solution
ll ldioph(ll a, ll b, ll c, ll &x, ll &y, ll &found) {
    ll g = extended_euclid(a, b, x, y);

    if((found = c % g == 0))
        x *= c / g, y *= c / g;

    return g;
}
```

Linear Diophantine equation

- Sometimes problems comes with variations to list all solutions with a restriction criteria.
  - Finding all solutions such that X in range [min_x; max_x] and Y in range[min_y; max_y]
  - Or some conditions restricting smallest sum of x + y
- For further notes about above 2 problems, see following russian page (translate lower parts)

Congruence

- Two integers a and b are called **congruent modulo n**, written $a \equiv b \pmod{n}$
  - It means a%n = b %n = x
  - Recall, this means (a-b) % n = 0
  - $37 \equiv 57 \pmod{10}$ $\qquad 37 - 57 = -20$
  - 37 %10 = 57 % 10 = 7. Also -20 % 10 = 0
  - More importantly: **a-b = qn** for some q integer (a = b+qn)
- if $ax \equiv ay \pmod{n}$ and gcd(a,n) = d, then the congruence is equivalent $x \equiv y \pmod{n/d}$
  - IF $ax \equiv ay \pmod{n}$ SAME as $x \equiv y \pmod{n}$ THEN d = 1
  - Reverse doesn't need this condition

Congruence Facts

- if $a \equiv b \pmod{m}$ $\quad a^n \equiv b^n \pmod{m}$ for all $n \geq 1$.
- If p is prime, $\quad (x+y)^p \equiv x^p + y^p \pmod{p}$.
- If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$.

  If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a \pm c \equiv b \pm d \pmod{m}$.

  If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $ac \equiv bd \pmod{m}$.

  If $a \equiv b \pmod{m}$, then $a + c \equiv b + c \pmod{m}$.

  If $a \equiv b \pmod{m}$, then $ca \equiv cb \pmod{m}$.
- From last one, $ax \equiv b \pmod{n}$ same as $x \equiv ba^{-1} \pmod{n}$

Congruence and large powers

- Find answer of 3^{5555} % 80
  - Hint: Think how to reduce the large power?!
  - Hint: $3^4 \equiv 1$ (% 80) and $5555 = 4 * 1388 + 3$
  - Then, 3^{5555} % 80 = 3^3 % 80 = 27
- Find answer of $(3^{1000} + 3)$ % 28
  - Hint: $3^3 = 27 = \mathbf{-1}$ (% 28) and $1000 = 3*333+1$
  - Then equation = [(-1 * 3) + 3] (% 28) = 0
- Your turn
  - prove that $2^{(5n+1)} + 5^{(n+2)} \equiv 0 \pmod{27}$

Linear Modular Equation

- Solve $ax \equiv b$ (% m)
- $258x \equiv 369 \mod 147$
  - $258x - 63 = 147y$ For some y integer
  - $258x + 147y = 63$ An **LD equation**
  - LDE has infinite solutions: $x = 492 - 147r / 3$
- % should impose some restrictions (duplicate)
  - We take %m to any ax, then we have m solutions max!
  - However, we can prove ONLY **gcd** unique solutions exist

Linear Modular Equation: Code

```
// solves the equation ax = b (mod n)
vector<ll> modularEquation(ll a, ll b, ll n)
{
    vector<ll> sols;
    ll x, y, g;
    g = extended_euclid(a, n, x, y);

    if(b % g != 0)
        return sols;    // no solutions

    x = ((x * b / g)%n + n)%n;  // from LDE, +ve mod

    for( int i = 0; i < g; ++i) // Bézout's identity
        sols.push_back( ( x + i * n / g ) % n );

    sort(sols.begin(), sols.end());
    return sols;
}
```

Your turn

- There are **Important** readings
- Linear Diophantine Equations
- Congruences and Modular Arithmetic
- Solving Linear Congruences
- Congruence .. read … solve
- Optional: Quadratic Equations

تم بحمد الله

علمكم الله ما ينفعكم

ونفعكم بما تعلمتم

وزادكم علماً

Problems

- SGU 106 (The equation), CodeforcesGym100506C(Cutting Banknotes), UVA (718, 11768)