OI Math Docs

目录

数论

GCD

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

```
int gcd(int a, int b) {
    return a == 0 ? b : gcd(b, a % b);
}
```

exGCD

求解 $ax + by = \gcd(a, b)$ 的一组特解 $\begin{cases} x = x_0 \\ y = y_0 \end{cases}$。

$$\text{exgcd}(a, b) \to (d, x_0, y_0)$$

```
void exgcd(int a, int b, int &d, int &x, int &y) {
    if (b == 0) d = a, x = 1, y = 0;
    else {
        exgcd(b, a % b, d, x, y);
        int t = x; x = y; y = t - a / b * y;
    }
}
```

二元一次不定方程

求解 $ax+by=c$ 的一组特解 $\begin{cases}x=x_0\\y=y_0\end{cases}$。

$$\begin{aligned}
&\operatorname{exgcd}(a,b)\to(d,x_0,y_0)\\
\Rightarrow\quad & ax_0+by_0=\gcd(a,b)\\
\Rightarrow\quad & a\frac{x0}{\gcd(a,b)}+b\frac{y0}{\gcd(a,b)}y=1\\
\Rightarrow\quad & a\frac{x_0c}{\gcd(a,b)}+b\frac{y_0c}{\gcd(a,b)}=c\\
\Rightarrow\quad & \begin{cases}x=\dfrac{x_0c}{\gcd(a,b)}\\[2ex] y=\dfrac{y_0c}{\gcd(a,b)}\end{cases}
\end{aligned}$$

有解条件： $c \bmod \gcd(a,b)=0$。

```
bool linearEquation(int a, int b, int c, int &x, int &y) {
    int d; exgcd(a, b, d, x, y);
    if (c % d) return false;
    int t = c / d;
    x *= t, y *= t;
    return true;
}
```

线性同余方程

求解 $ax \equiv b \pmod c$ 的最小正整数解。

$$
\begin{aligned}
& ax \equiv b \pmod c \\
\Rightarrow \quad & ax + cy = b \\
\Rightarrow \quad & \text{linearEquation}(a, c, b) \to (x, y)
\end{aligned}
$$

有解条件：$b \bmod \gcd(a, c) = 0$。

```
int equiv(int a, int b, int c) {
    int x, y;
    if (linearEquation(a, c, b, x, y)) {
        int t = gcd(a, c);
        return (x % t + t) % t;
    } else return -1;
}
```