最大公因数，最小公倍数

GCD, LCM

欧几里得算法 Euclidean Algorithm

Theorem：

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

Proof：设 $a=kb+c$，则 $c=a \bmod b$。设 $d=\gcd(a,b)$，则 $d\mid a, d\mid b$，故 $d\mid c$；反过来，若 $d\mid b, d\mid c$，则 $d\mid a$.

Theorem：

$$\gcd(a,b)\times \mathrm{lcm}(a,b)=a\times b$$

Proof：由**唯一分解定理**易证。

Complexity：$O(\lg n)$

Code：

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

int lcm(int a, int b){
    return a / gcd(a, b) * b;
}
```

扩展欧几里得算法 Extended Euclidean Algorithm

贝祖定理 Bézout's identity：方程 $ax+by=c$ 有整数解当且仅当 $\gcd(a,b)\mid c$.
Proof：暂略。

Theorem：用扩展欧几里得算法可以求出 $ax+by=d$（其中 $d=\gcd(a,b)$）的一组特解。
Proof：因为 $a \bmod b = a - b\times\left\lfloor\frac{a}{b}\right\rfloor$，在欧几里得算法的一层上，设有 $ax+by=d$，则有 $\left[a \bmod b + b\times\left\lfloor\frac{a}{b}\right\rfloor\right]\cdot x+by=d$，故 $b\times\left(\left\lfloor\frac{a}{b}\right\rfloor\cdot x+y\right)+(a \bmod b)\cdot x=d$，即在欧几里得算法的下一层上，有 $\begin{cases}x'=\left\lfloor\frac{a}{b}\right\rfloor\cdot x+y\\y'=x\end{cases}$，即 $\begin{cases}x=y'\\y=x'-\left\lfloor\frac{a}{b}\right\rfloor\cdot y'\end{cases}$. 每次回溯时更改即可。
边界：$a=d,b=0$ 时，取 $x=1,y=0$.

上述过程求得 $ax+by=d$ 的一组特解 x_0,y_0，该方程的**通解**为：$\begin{cases}x=x_0+kb\\y=y_0-ka\end{cases}(k\in\mathbb{Z})$

Application：

- 解 $ax+by=c$：有解时，根据贝祖定理，c 是 $\gcd(a,b)$ 的倍数，于是解出 $ax+by=\gcd(a,b)$ 后，x,y 乘上 $\frac{c}{\gcd(a,b)}$ 即可。
- 求解逆元：已知 a,b，求满足 $ax\equiv1\pmod b$ 的 x。当 a,b **互质**时，原式等价于求解 $ax+by=1$。

Code：

```
int exgcd(int a, int b, int &x, int &y){ // solve ax+by=gcd(a,b)
    if(b == 0){
        x = 1;
        y = 0;
        return a;
    }
    int d = exgcd(b, a % b, x, y);
    int t = x;
    x = y;
    y = t - a / b * y;
    return d;
}
```