

快速幂

取模运算: $a \bmod p$ 表示 a 除以 p 的余数

The top screenshot shows a whiteboard with the following content:

$a^k \bmod p$

log k {

- $a^{2^0} \bmod p$
- $a^{2^1} \bmod p$
- $a^{2^2} \bmod p$
- \vdots
- $a^{2^{\log k}} \bmod p$

a^k

$= a^{2^{x_1}} \cdot a^{2^{x_2}} \cdots a^{2^{x_t}}$

$= a^{2^{x_1} + 2^{x_2} + \cdots + 2^{x_t}}$

www.acwing.com

The bottom screenshot shows a whiteboard with the following content:

$4^5 \bmod 10$

$(5)_2 = (101)_2$

$4^5 = 4^{(101)_2}$

$= 4^{2^0 + 2^2}$

$= 4^{2^0} \cdot 4^{2^2}$

$= 4 \times 6$

$\equiv 4 \pmod{10}$

$4^{2^0} \equiv 4 \pmod{10}$

$4^{2^1} \equiv 6 \pmod{10}$

$4^{2^2} \equiv 6 \pmod{10}$

www.acwing.com

以下为y总代码:

```
#include
#include

using namespace std;

typedef long long LL;
```

```

LL qmi(int a, int b, int p)
{
    LL res = 1 % p;
    while (b)
    {
        if (b & 1) res = res * a % p;
        a = a * (LL)a % p;
        b >>= 1;
    }
    return res;
}

int main()
{
    int n;
    scanf("%d", &n);
    while (n -- )
    {
        int a, b, p;
        scanf("%d%d%d", &a, &b, &p);
        printf("%lld\n", qmi(a, b, p));
    }
}

```

```
return 0;
```

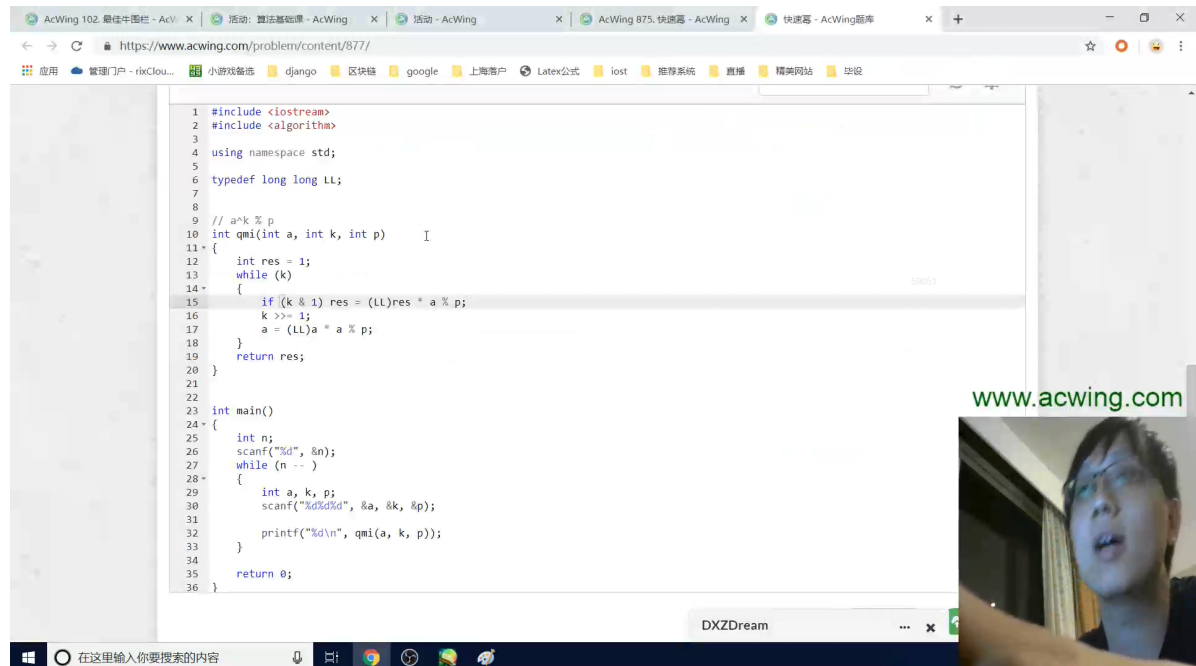
```
}
```

作者: yxc

链接: <https://www.acwing.com/activity/content/code/content/50237/>

来源: AcWing

著作权归作者所有。商业转载请联系作者获得授权，非商业转载请注明出处。



对于 a^b 来说, 若果把 b 写成2 进制, 那么 b 就可以写成若干二次幂之和, 如13 的二进制 1101, 于是 3 号位、2号位、0号位就都是1, 那么就可以得到 $13 = 2^3 + 2^2 + 2^1 = 8 + 4 + 1$ 。所以 $a^{13} = a^8 * a^4 * a^1$ 。

通过同样的推导，我们可以把任意的 a^b 表示成 $a^{(2^k)}$、 a^8 、 a^4 、 a^2 、 a^1 中若干的乘积。若果二进制的 i 号为1.那么想中的 $a^{(2^i)}$ 就被选中。于是可以得到计算 a^b 的大致思路：令 i 从0到 k 枚举 b 的二进制的每一位，如果为1 那就累计 $a^{(2^i)}$ 。注意

$a^{(2^k)}$、 a^8 、 a^4 、 a^2 、 a^1 前一项总是等于后一项的平方。具体步骤。

- (1) 初始令 $ans = 1$,用来存放累积的结果。
- (2) 判断 b 的二进制末尾是否为1，（及判断 $b \& 1$ 是否为 1），也可以理解为判断 b 是否为奇数。如果是的话，令 ans 乘上 a 的值。
- (3) 令 a 平方，并使 b 右移一位，（也可以理解为， $b/2$ ）
- (4) 只要 b 大于0，就返回（2）。

```
1 typedef long long ll
2 ll binaryPow(ll a, ll b, ll m){
3     ll ans = 1;
4     while(b > 0){
5         if(b & 1){
6             ans = ans * a % m;
7         }
8         a = a * a % m;
9         b >>= 1;
10    }
11    return ans;
12 }
```

例： a^{13}

b	b&1	ans	a
		1	a
1101	1	1*a=a	a^2
110	0	a	a^4
11	1	$a*a^4 = a^5$	a^8
1	1	$a^5 * a^8 = a^{13}$	