Miller-Rabin素性测试

费马素性测试

根据**费马小定理**：若 p 是素数且 $\gcd(a,p)=1$，则 $a^{p-1}\equiv 1 \pmod p$.

要测试数 n 是否是素数，就随机在 $[1,n-1]$ 之中选择一个数 a，检验费马小定理是否成立。

然而费马小定理逆定理是不成立的，所以我们需要多次随机。

卡迈克尔数

费马素性测试在卡迈克尔数处失效。

对于合数 n，若对于所有与之互质的数 a，都有 $a^{n-1}\equiv 1 \pmod n$，则称 n 为卡迈克尔数 $\textbf{Carmichael number}$，又称费马伪素数。

二次探测定理

对于素数 p，$x^2\equiv 1 \pmod p$ 在模 p 意义下有且仅有两个解：$x=\pm 1$.

证：$x^2\equiv 1 \pmod p \iff p\mid x^2-1 \iff p\mid (x-1)(x+1)$，由于 p 是素数，故只能是 $x\pm 1\equiv 0 \pmod p$，即 x 在模 p 意义下仅有两解 $x\equiv \pm 1 \pmod p$. $\square$

Miller-Rabin

结合使用费马小定理和二次探测定理。

将 $n-1$ 分解为 $n-1=u\times 2^t$，设 $v=a^u$，那么如果 n 是素数，由费马小定理有：

$$a^{n-1}\equiv a^{u\times 2^t}\equiv v^{2^t}\equiv 1 \pmod n$$

再由二次探测定理可知：要么 $v\equiv \pm 1 \pmod n$，要么 $\exists t'<t$，使得 $v^{2^{t'}}\equiv -1 \pmod n$.

如果 n 是卡迈克尔数——使得费马素性测试失效的数呢？那它就逃不过二次探测了。

Code

```
mt19937 rnd(time(NULL));
namespace Miller_Rabin{

    LL fpow(LL bs, LL idx, LL mod){
        bs %= mod;
        LL res = 1;
        while(idx){
            if(idx & 1) (res *= bs) %= mod;
            (bs *= bs) %= mod;
            idx >>= 1;
        }
        return res;
    }
    bool test(LL n){
        if(n < 3)   return n == 2;
        if(!(n & 1))    return false;
        LL u = n - 1, t = 0;
        while(u % 2 == 0)   u /= 2, t++;
        int testTime = 10;
        while(testTime--){
            LL v = rnd() % (n - 2) + 2;
            v = fpow(v, u, n);
            if(v == 1 || v == n - 1)    continue;
            int j; for(j = 0; j < t; j++, v = v * v % n)
                if(v == n - 1)  break;
            if(j >= t)  return false;
        }
        return true;
    }
}
```