二进制的哈希中的求余

2022 年 8 月 16 日

1. 设 a，b 为正整数，我们用 $a \mod b$ 表示 a 除以 b 取余数得到的值。在数论中，我们有如下结论。

   (a) $(a+b) \mod p = ((a \mod p) + (b \mod p)) \mod p$。

   (b) 设 k 和 p 为正整数，则

   $$2^k \mod p = 2 \cdot (2^{k-1} \mod p) \mod p。$$

   设 $p = 10^9 + 7$，编写程序完成如下任务（要求程序只使用 `unsigned long long` 型的变量或者数组）。

   (a) 计算从 $2^0 \mod p$，$2^1 \mod p$ 到 $2^{1023} \mod p$ 的值（无需输出）。

   (b) 输出 $2^5 \mod p$，$2^{17} \mod p$，$2^{567} \mod p$ 和 $2^{1021} \mod p$ 的值。

   (c) 计算 $(2^5 + 2^{17} + 2^{567} + 2^{1021}) \mod p$ 的值并输出。

   提示：

   (a) 设置一个包含 1024 个元素的数组，其中 `a[k]` 表示 $(2^{\mathtt{k}} \mod p)$ 的值。

   (b) `a[k+1]` 和 `a[k]` 的值有何递推关系（其中 $\mathtt{k} \geq 1$）?

   (c) $2^5 \mod p$，$2^{17} \mod p$，$2^{567} \mod p$ 和 $2^{1021} \mod p$ 的值应该如何从数组中获得?

   (d) $(2^5 + 2^{17} + 2^{567} + 2^{1021}) \mod p$ 如何展开？如何化归到上一问?

   参考结果：

```
2^5 mod 1000000007: 32
2^17 mod 1000000007: 131072
2^567 mod 1000000007: 84031934
2^1021 mod 1000000007: 101591824
final res: 185754862
```

```c
#include <stdio.h>
int main()
{
    unsigned long long p = 1000000007;
    unsigned long long a[1023];
    a[0] = 1;
    for(int k = 1; k < 1024; k++)
    {
        a[k] = (2 * a[k - 1]) % p;
    }
    unsigned long long res = (a[7] + a[17] + a[579] + a[1023]) % p;
    printf("%llu", res);
    return 0;
}
```