数论基础选讲

山东省实验中学

宁华

问题引入：

- 求正整数 3^{83} 的最后两位数

- 看到类似这样求一个数的某次方的最后几位数的问题，没有接触过初等数论的同学可能第一反应是小学的做法：找规律。

- 可以看出来 3^n 的个位是 1,3,9,7 循环，循环周期是 4

- 而十位是 $0, 0, 0, 2, 8, 4, 2, 8, 6, 8, 4, 4, 4, 2, 6, 0, 2, 6, 8, 6$ 循环，
- 循环周期是 20

- 所以 3^83 最后两位是 27

$$
\begin{aligned}
3^0 &= 1 \\
3^1 &= 3 \\
3^2 &= 9 \\
3^3 &= 27 \\
3^4 &= 81 \\
3^5 &= 243 \\
3^6 &= 729 \\
3^7 &= 2187 \\
3^8 &= 6561
\end{aligned}
$$

- 接触过一点初等数论的同学表示这种方法too young，因为这个问题可以用欧拉定理(Euler's theorem)秒杀。

欧拉定理(Euler's theorem)

- 若a,p互质，则有

$$a^{\varphi(p)} \equiv 1 \pmod p$$

- 其中欧拉函数 φ(p) 是小于 p 的正整数中和 p 互质的数的个数.

- 可以看出，费马小定理其实是欧拉定理的特例。

- 回到问题引入：求正整数 3^83 的最后两位数
- 即求 3^83%100

- 发现3与100互质，所以3^φ(100)%100=1
- φ(100)=100*(1-1/2)*(1-1/5)=40
- 3^83=(3^40)^2 * 3^3
- 3^83%100=3^3%100=27

习题

- 求 $2014^{2014^{2014}}$ 的最后两位数
- 求 $1^{2016}+2^{2016}+\cdots+2016^{2016}$ 除以 2016 的余数
- 求 $8^{7^{6^{5^{4^{3^{2^{1}}}}}}}$ 的最后三位数
- 有多少个正整数 $1\le n\le 2015$ 使得 n^{n^n} 和 n^n 的个位数相同？
- 249 的奇数次方末尾总会出现其本身 $249^3=15438249$，
- $249^5=957186876249$ 等等。1000 以内有多少个正整数有这样的性质？

威尔逊定理

- 威尔逊定理是以英格兰数学家爱德华·华林的学生约翰·威尔逊命名的，尽管这对师生都未能给出证明。华林于1770年提出该定理，1773年由拉格朗日首次证明。

- 威尔逊定理是判定一个自然数是否为素数的充分必要条件

一个实验

- 十八世纪中叶，一位英国法官约翰·威尔逊爵士，发现了数论中一种极为罕见的关系：取从1到某个质数所有连续正整数的乘积，例如从1乘到11，即11的阶乘11！。显然，11！能被从1到11的所有整数整除，除去11这个数，得10！。无疑10！不能被11整除。

- 然而，如果给10！加上1的话，1×2×3×4×5×6×7×8×9×10＋1＝3628801，怎么也不会想到，3628801却能被11整除（3628801÷11＝329891）。
- 类似地，从1到质数7的阶乘7！中略去7，再加上1，得1×2×3×4×5×6＋1＝721，721也能被7整除（721÷7＝103）

11 和 7 都是质数，研究发现，此种整除性对一切质数都成立，但对合数却不成立。下面的表格展示了这一规律：

n	(n-1)!	(n-1)!+1	[(n-1)!+1] mod n	数性
2	1	2	0	质数
3	2	3	0	质数
4	6	7	3	合数
5	24	25	0	质数
6	120	121	1	合数
7	720	721	0	质数
8	5040	5041	1	合数
9	40320	40321	1	合数
10	362880	362881	1	合数
11	3628800	3628801	0	质数
12	39916800	39916801	1	合数
13	479001600	479001601	0	质数
14	6227020800	6227020801	1	合数
15	87178291200	87178291201	1	合数

威尔逊定理

- 威尔逊定理：
- 当p为质数时，(p-1)! + 1 能被p整除。

- 威尔逊定理逆定理：
- 若一个数 (p-1)! + 1 能被 p 整除，那么 p 为质数

- p 为质数 $\Longleftrightarrow (p-1)! \equiv -1 \pmod p$

HDU 2973 YAPTCHA

【题意模型】:

对于给定的数 i，求 Si 的值，其中：

$$S_n = \sum_{k=1}^{n} \left\lfloor \frac{(3k+6)!+1}{3k+7} - \left\lfloor \frac{(3k+6)!}{3k+7} \right\rfloor \right\rfloor$$

核心代码参考

```
#define M 3000008
int s[M];
bool isprime[M];
void shai()
{
......
}
```

```
int main()
{
    shai();
    for (int i = 2; i < M / 3; ++i) s[i] = s[i - 1] + (isprime[i * 3 + 7] ? 1 : 0);
    int T; scanf("%d", &T);
    while (T--)
    {
        int n; scanf("%d", &n); printf("%d\n", ans[n]);
    }
    return 0;
}
```