初等数论自测题三 参考答案与评分标准

一、名词解释

1. Given m integers $\{a_1, a_2, \cdots, a_m\}$, if $\{\overline{a_1}, \overline{a_2}, \cdots, \overline{a_m}\} = \{\overline{0}, \overline{1}, \cdots, \overline{m-1}\}$ (modulo m sense), then $\{a_1, a_2, \cdots, a_m\}$ is called a complete residue system modulo m. ……………3 分

（注：模 m 的完全剩余系的定义形式不唯一，有若干等价的定义。）

2. Let m be a positive integer, a is an integer coprime to m, the order of a modulo m is the least positive integer r, s.t. $a^r \equiv 1(mod\ \ m)$. ………………………………3 分

3. Euler's Theorem:
Let m be a positive integer, a is an integer coprime to m, then

$$a^{\phi(m)} \equiv 1(mod\ \ m)$$

…………………………………4 分

二、应用题

4.
Sol:
Yes, it is possible. ………………………………………3 分
The algorithm is the so called "repeated squaring method":
First, write out the binary presentation of b=2017201820192020, it's just divide b by 2 repeatedly, thus takes no time. ………………………………………3 分

Now, suppose we already know $x^{2^i}(mod n)$, which should be a 20-digit number, then we square it to get a 40-digit number and then divide the result by n, all these cost at most 2 seconds, we then get $x^{2^{i+1}}(mod n)$, thus by induction, we could get $x^{2^i}(mod n)$ for all $i < k$ in *2k* seconds. ………………………………………3 分

Now multiply all $x^{2^i}(mod n)$ if the i-th digit in the binary presentation is 1 in the same way as above: multiply the first 2 numbers and then divide it by n, and then multiply the result with the 3rd number and then divide it by n...... …………………………3 分

Thus the total time is at most 4k where $k = [log_2 b] < 70$, so we can finish the computation in 5 minutes. In fact, an upper bound of the time is 200 seconds. ………………3 分

三、计算题

5.

Sol:

a) $\phi(1000000)=(2^6-2^5)\times(5^6-5^5)=400000$， so the number of integers between 0 and 1000000 that are coprime to 1000000 is 400000. ……………………………………5 分

b)参考课上例题写出求解过程，注意和 1000000 互素的数其实就是和 10 互素的数。

The number of integers between 0 and 2022 that are coprime to 1000000 is 809.

……………………………………5 分

6.

Sol:

We calculate $2021^{12306}(mod\, 8^4)$ first.

Since 2021 is coprime to 8^4, and $\phi(8^4)=\phi(2^{12})=2^{11}=2048$, by Euler's theorem

$2021^{2048}\equiv 1(mod\, 8^4)$. ………………………………4 分

So, Use repeated Squaring Method（自行补完过程），

$2021^{12306}\equiv 2021^{18}\equiv 665(mod\, 8^4)$, i.e. $2021^{12306}(mod\, 8^4)=665$.

………………………………3 分

（注：也可直接使用反复平方法计算 $2021^{12306}(mod\, 8^4)$，但过程较为冗繁。）

Now, convert 665 to octal representation（自行补完过程）, we get the last four digits of the octal representation of 2021^{12306} are $(1231)_8$. ………………………………3 分

7.

Sol:

a) Yes, there is a primitive root modulo 250. ……………………………………1 分

In fact, there is a primitive root modulo n if and only if n is one of the following: 2,4, p^l， $2p^l$ where p is an odd prime. Now, since $250=2\times 5^3$, so there is a primitive root modulo 250. ……………………………………3 分

b) 参考课上例题写出过程

3 is a primitive root modulo 250.

……………………………………过程 5 分、答案 1 分

8.

Sol:

a) 参考课上例题写出过程

The order of 2021 modulo 108108 is 180.

……………………………………过程 5 分，答案 2 分

b) By part a), $2021^{180} \equiv 1(mod 108108)$ ……………………………………2 分

Thus $2021^{1800}(mod 108108) = 1$. ……………………………………1 分

（注：b)小问也可不利用 a)小问的结论直接求解：可以用反复平方法直接计算、也可以用欧拉定理、费马小定理、中国剩余定理结合反复平方法计算。）

四、证明题

9.

Proof：

Note that $n, n+1, n+2$ is a complete residue system modulo 3. ………………2 分

Thus $n^2+(n+1)^2+(n+2)^2 \equiv 0^2+1^2+2^2 \equiv 2(mod\ \ 3)$. ………………3 分

But the remainder of every square divided by 3 is either 0 or 1.

Thus $n^2+(n+1)^2+(n+2)^2$ can't be a square. ………………3 分

10.

Proof：

a)

127 is a prime. ……………………………………………………………2 分

In fact, $[\sqrt{127}] = 11$, to verify 127 is a prime or not, we just need to let 2,3,5,7,11 to divide 127. ……………………………………………………检验过程 3 分

b)

By Fermat's little theorem, for any integer a coprime to 127,

$$a^{126} \equiv 1(mod 127)$$ ……………………………………………………2 分

c)

1729 is a composite. ……………………………………………………………1 分

$1729 = 7 \times 13 \times 19$. ……………………………………………………………2 分

d)

Since a coprime to 1729, a coprime to 7, 13, 19 respectively. ………………1 分

By Fermat's little theorem,

$$a^6 \equiv 1(mod 7)$$ ……………………………………………………2 分

$a^{12} \equiv 1 (mod 13)$ ……………………………………………………2 分

$a^{18} \equiv 1 (mod 19)$ ……………………………………………………2 分

Thus

$a^{1728} \equiv 1 (mod 7)$

$a^{1728} \equiv 1 (mod 13)$

$a^{1728} \equiv 1 (mod 19)$

……………………………………………………………………1 分

So 7,13,19 are divisors of $a^{1728} - 1$, and they are pairwise coprime, thus

$a^{1728} \equiv 1 (mod 1729)$. ……………………………………………………………………2 分

11.
Proof:

$2^{251} - 1$ is a composite number. ……………………………………………………2 分

Use repeated squaring method, we can get $2^{251} \equiv 1 (mod 503)$.

…………………………反复平方法的过程 4 分

So 503 is a prime factor of $2^{251} - 1$, $2^{251} - 1$ is a composite number.

……………………………………………………1 分

（注：关于 503 这个素因子是怎么找到的，请参考上课内容）

关于本题的一点历史注记：

1984 年，美国计算机协会（ACM）为纪念美国电子工程学会（IEEE）一百周年作了一个纪念碑，上面刻有$2^{251} - 1$*的素因子分解式。ACM 主席还做了以下注解：*

"大约三百年前，法国数学家梅森预言$2^{251} - 1$*是合数，大约一百年前证明了它的确是合数，但直到 20 年前还被认为没有进行分解的计算装置。事实上，用通常的计算机和传统算法，分解它的计算时间预估是*10^{20} *年。今年 2 月，这个数在 Sandia 的 Cray 计算机上用 32 小时被分解成功。这是一个世纪的记录，我们在计算方面已走了很长的路程，为了纪念 IEEE 对计算的贡献，在这里刻上这个梅森数的 5 个素因子。*