2019-2020A卷

一、计算题（共 6 小题，每小题 10 分，共 60 分）

1. 已知 $a=527, b=1411$，求最大公因子(a,b)和最小公倍数$[a,b]$。

解：

由辗转相除法：

$$
\begin{aligned}
527 &= 0 \times 1411 + 527 \\
1411 &= 2 \times 527 + 357 \\
527 &= 1 \times 357 + 170 \\
357 &= 2 \times 170 + 17 \\
170 &= 10 \times 17 + 0
\end{aligned}
$$

$\therefore\ (527, 1411) = 17$

而

$$
[a,b] = \frac{ab}{(a,b)} = \frac{527 \times 1411}{17} = 43741
$$

$\therefore\ [527, 1411] = 43741$

2. 利用勒让德符号判断同余方程 $x^2 \equiv 30 \pmod{41}$是否有解?

解：

勒让德符号为

$$\left(\frac{30}{41}\right)=\left(\frac{2}{41}\right)\left(\frac{5}{41}\right)\left(\frac{3}{41}\right)$$

$$\left(\frac{2}{41}\right)=(-1)^{\frac{40\times 42}{8}}=1$$

$(5,41)=1 \qquad (3,41)=1,$ 由二次互反律

$$\left(\frac{5}{41}\right)=(-1)^{\frac{4}{2}\frac{40}{2}}(\frac{1}{5})=1$$

$$\left(\frac{3}{41}\right)=(-1)^{\frac{2}{2}\frac{40}{2}}(\frac{2}{3})=-1$$

$$\therefore \left(\frac{30}{41}\right)=1\cdot 1\cdot(-1)=-1$$

$\therefore$ 30不是模41的平方剩余，原式无解。

3. 求乘法群$\mathbf{F}_{23}^*$的所有生成元。

解：

$\mathbf{F}_{23}^*=(Z/23Z)^*$为模23的简化剩余系

$\varphi(23)=22$，因此群阶为22.

由原根g性质，$g,g^2,\cdots,g^{\varphi(m)}$构成模$m$的简化剩余系

$\therefore$ 23的原根$g=5$为一个$\mathbf{F}_{23}^*$生成元

一共有$\varphi(22)=10$个生成元，形式为$g^j,(j,22)=1$

$j=1,3,5,7,9,13,15,17,19,21$

$\therefore$ 生成元g^j为$5,10,20,17,11,21,19,15,7,14.$

4. 求解同余式组

$$\begin{cases} x \equiv 2 \pmod 3 \\ 3x \equiv 4 \pmod 5 \\ x \equiv 4 \pmod 7 \end{cases}$$

解：

解 $3x \equiv 4 \pmod 5$，得 $x \equiv 3 \pmod 5$

因此原同余式组等价为

$$\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5 \\ x \equiv 4 \pmod 7 \end{cases}$$

由CRT,

$m = 3 \times 5 \times 7 = 105$

$M_1 = 5 \times 7 = 35 \qquad M_1^{'} = 2$

$M_2 = 3 \times 7 = 21 \qquad M_2^{'} = 1$

$M_3 = 3 \times 5 = 15 \qquad M_3^{'} = 1$

$\therefore$ 原同余式组的解为$x \equiv 2 \times 35 \times 2 + 3 \times 21 + 4 \times 15 \pmod{105}$

$\therefore x \equiv 53 \pmod{105}$

5. 求解同余式 $f(x) = 3x^4 + 17x^3 - 5x + 23 \mod 25$

解：

(1) $f'(x) = 12x^3 + x^2 + 20 \mod 25$;
(2) 验证 $f(x) = 3x^4 + 2x^3 + 3 \mod 5$ 的解为 $x_1 = 3 \mod 5$;
(3) 将 $x = 3 + 5t$ 代入方程

$$f(3) + f'(3) \cdot t \cdot 5 \equiv 0 \mod 25;$$

而$f(3) \equiv 10 \mod 25$，$f'(3) \equiv 3 \mod 25$，也即

$$10 + 3 \cdot t \cdot 5 \equiv 0 \mod 25 \text{ 或 } 2 + 3 \cdot t \equiv 0 \mod 5$$

解得 $t \equiv 1 \mod 5$，所以 $x = 3 + 5t \equiv 8 \mod 25$。

6. 假设椭圆曲线 $y^2 = x^3 + 5x + 3 \pmod{11}$上的两点 $P = (x_1, y_1), Q = (x_2, y_2)$ 之和为 $P_3 = (x_3, y_3) = P + Q \neq O$ 的计算公式为

$$x_3 = \lambda^2 - x_1 - x_2, \quad y_3 = (x_1 - x_3)\lambda - y_1$$

其中 ① $x_1 \neq x_2$时，$\lambda = \frac{y_2 - y_1}{x_2 - x_1}$，② $x_1 \neq x_2$，且$Q \neq -P$时，$\lambda = \frac{3x_1^2 + 5}{2y_1}$.

若$P = (3, 1)$，试求$3P$。

解：

首先计算 $2P$，因为

$$\lambda = \frac{3x_1^2 + 5}{2y_1} = \frac{3 \times 7^2 + 5}{2 \times 4} = 8;$$

所以

$$\begin{aligned} x_3 &= \lambda^2 - x_1 - x_2 = 16^2 - 3 - 3 = 250 \equiv 8 \pmod{11}; \\ y_3 &= (x_1 - x_2)\lambda - y_1 = (3 - 250) \times 16 - 1 = -3953 \equiv 7 \pmod{11} \end{aligned}$$

故 $2P = (8, 7)$;

同理计算 $3P = 2P + P = (8, 7) + (3, 1)$，其中

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} = 10;$$

因此容易得 $3P = 2P + P = (8, 7) + (3, 1) = (1, 8)$。

二、 证明题（共 10 分）

假定 a 和 b 是一个群 G 的两个元，并且 $ab = ba$。又假定 a 的阶是 m， b 的阶是 n ，并且$(m, n) = 1$。证明：ab 的阶是 mn。

证明：

G 是一个群，$a, b \in \mathrm{G}$，$ab = ba$，由群封闭性，$ab \in \mathrm{G}$.

设 ab 的阶为 k，$(ab)^k = e$.

根据题干，$a^m = b^n = e$，因此$(a^m)^n (b^n)^m = e$.

由群元阶的性质：$k \mid mn$.

而$(ab)^k = a^k b^k = e$. 所以b^k 也是 a^k 的逆元.

设 a 的逆元 a^{-1}，于是 $(aa^{-1})^k = e = a^k a^{-k}$.

所以 $(a^{-1})^k = a^{-k}$ 也是 a^k 逆元. 根据群逆元的唯一性，$b^k = a^{-k}$.

所以 $(b^n)^k = b^{kn} = (a^{-k})^n$，注意到 $b^n = e$.

所以 $a^{-kn} = e$.

所以 $m \mid (-kn) \Leftrightarrow m \mid kn$，又根据题干 $(m, n) = 1$.

所以 $(m, kn) = (m, k) = m \Rightarrow m \mid k$.

同理，a^k 也是 b^k 的逆元，于是 $a^k = b^{-k}$，由 $a^m = e \Rightarrow a^{km} = b^{-km} = e$.

所以 $n \mid km, \quad (n, km) = n$，又 $(m, n) = 1, \quad (n, km) = (n, k) = n \Rightarrow n \mid k$.

由于 $m \mid k, \quad n \mid k$，所以 $[m, n] \mid k$.

而 $(m, n) = 1$，因此 $[m, n] = mn$，所以 $mn \mid k$.

又之前有 $k \mid mn, \quad mn \mid k$,

$\therefore k = mn$. 综上，ab 的阶 $k = mn$.

三、应用题（每小题 15 分，共 30 分）

1. 构造有限域 $GF(16) = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15\}$（其中模多项式为$m(x) = x^4 + x + 1$ 的加法表和乘法表。（填表即可）

加法表

$\oplus$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0																
1																
2																
3																

乘法表

$\otimes$	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
0																
1																
2																
3																

解：

$\oplus$	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
0	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	1	0	3	2	5	4	7	6	9	8	11	10	13	12	15	14
2	2	3	0	1	6	7	4	5	10	11	8	9	14	15	12	13
3	3	2	1	0	7	6	5	4	11	10	9	8	15	14	13	12

乘法表

$\otimes$	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
2	0	2	4	6	8	10	12	14	3	1	7	5	11	9	15	13
3	0	3	6	5	12	15	10	9	11	8	13	14	7	4	1	2

2.著名 RSA 公钥密码加密系统如下：

① 随机选择两个大素数 p 和 q，而且保密；

② 计算 $n=pq$，将 n 公开；

③ 计算欧拉函数 $\varphi(n)=(p-1)(q-1)$，并对 $\varphi(n)$ 保密；

④ 随机选取正整数 $e\in(1,\varphi(n))$ 且有 $(e,\varphi(n))=1$，并将 e 公开；

⑤ 根据 $ed\equiv 1 \mod \varphi(n)$，求出 d，并对 d 保密；

⑥ 加密运算：$C=M^e \mod n$；⑦ 解密运算：$M=C^d \mod n$。

现令公钥 $n=133,e=101$。问：（1）若待加密的明文 $M=83$，求相应的密文 C；（2）若待加密的明文 $C=131$，求相应的密文 M

解：

(1)

密文$C = M^e \mod n = 83^{101} \mod 133 = 125;$

用反复平方法计算，$101 = (1100101)_2$

(1) $n_0 = 1,\ a_0 = 83,\ b_1 = 83^2 \equiv 106 \pmod{133}$

(2) $n_1 = 0,\ a_1 = a_0 = 83,\ b_2 = b_1^2 \equiv 64$

(3) $n_2 = 1,\ a_2 = a_1 \times b_2 = 125,\ b_3 = b_2^2 \equiv 106$

(4) $n_3 = 0,\ a_3 = a_2 = 125,\ b_4 = b_3^2 \equiv 64$

(5) $n_4 = 0,\ a_4 = a_3 = 125,\ b_5 = b_4^2 \equiv 106$

(6) $n_5 = 1,\ a_5 = a_4 \times b_5 = 83,\ b_6 = b_5^2 \equiv 64$

(7) $n_6 = 1,\ a_6 = a_5 \times b_6 = 125$

(2) 首先用广义欧几里得算法求出私钥 $d = 77$；则相应的明文$M = C^d \mod n = 131^{77} \mod 133 = (-2)^{77} \mod 133 = 101$。