2017-2018_2_A卷

一、计算题（每小题10分，共60分）。

1. 进制转换：

（1）将二进制$(10100101)_2$分别转换为十进制和十六进制；

（2）将十进制$(153)_{10}$分别转换为二进制和十六进制

解：

$$
\begin{aligned}
(10100101)_2 &= (165)_{10} = (A5)_{16} \\
(153)_{10} &= (10011001)_2 = (99)_{16}
\end{aligned}
$$

2. 2018**年6月**27**日是星期三，问过**$2^{20180628}$**天后是星期几？**

解：

对于星期，7天一周期；

$$2^{20180628} \pmod 7 = 1;$$

所以是星期四。

3. 求群$(Z/23Z)^* = \{1, 2, \cdots, 22\}$**的所有生成元。**

解：

$(Z/23Z)^*$ 是模 23 的简化剩余系，
对于乘法 $\otimes : a \otimes b = a \cdot b \pmod{23}$ 构成群。

而23是素数，所以 $\varphi(23) = 22$，而根据原根g的性质, $\{g^0, g, \cdots, g^{\varphi(23)-1}\}$ 构成模23的简化剩余系。

查原根表得到模23的原根有$g = 5$，因此5是一个生成元。

由于群阶22，所以$(Z/23Z)^*$有$\varphi(22) = 10$个生成元。

生成元形如$g^j, (j, 22) = \frac{22}{22} = 1, j = 1, 3, 5, 7, 9, 13, 15, 17, 19, 21$。

所以生成元是$g^j \pmod{23} = 5, 10, 20, 17, 11, 21, 19, 15, 7, 14$。

4. 求解同余式组

$$
\begin{cases}
x & \equiv 2 \pmod 9 \\
3x & \equiv 4 \pmod 5 \\
4x & \equiv 3 \pmod 7
\end{cases}
$$

解：

注意到9，5，7两两互素，但是方程左边不相同。

$3x \equiv 4 \pmod 5$，解得$x \equiv 3 \pmod 5$

$4x \equiv 3 \pmod 7$，解得$x \equiv 6 \pmod 7$

因此原方程组化为:

$$
\begin{cases}
x & \equiv 2 \pmod 9 \\
x & \equiv 3 \pmod 5 \\
x & \equiv 6 \pmod 7
\end{cases}
$$

由9，5，7两两互素,可运用中国剩余定理：

$$
\begin{aligned}
&M_1 = 35, M_1' = 8, \\
&M_2 = 63, M_2' = 2, \\
&M_3 = 45, M_3' = 5; \\
&m = m_1 m_2 m_3 = 315
\end{aligned}
$$

原方程组的解就是

$$
\begin{aligned}
&x \equiv 2 \cdot 35 \cdot 8 + 3 \cdot 63 \cdot 2 + 6 \cdot 45 \cdot 5 = 2288 \pmod{315} \\
&x \equiv 83 \pmod{315}
\end{aligned}
$$

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分
（2）验证 $f(x) = 3x^4 + 2x^3 + 3 \mod 5$ 的解为 $x_1 = 3 \mod 5;$　　　2分
（3）将 $x = 3 + 5t$ 代入方程

$$f(3) + f'(3) \cdot t \cdot 5 \equiv 0 \mod 25; \qquad 2分$$

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$y^2 = x^3 + 5x + 1 \pmod{11}$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$P = (7, 4)$，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

$$x_3 = \lambda^2 - x_1 - x_2 = 8^2 - 7 - 7 = 6;$$
$$y_3 = (x_1 - x_2)\lambda - y_1 = (7 - 6) \times 8 - 4 = 4$$

故 $2P = (6, 4)$;

同理计算 $3P = 2P + P = (6, 4) + (7, 4)$，其中

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} = 0;$$

因此容易得 $3P = 2P + P = (6, 4) + (7, 4) = (9, 7)$。

二、证明题（每小题10分，共20分）。

1. 证明：阶是p^m的群（p是素数）一定包含一个阶是p的子群。

证明：

任取阶为 p^m 的群 G

$\because p$ 是素数

$\therefore p^m > 1$

$\therefore \exists a \in G,\ a \neq e$

令 $H=(a)$，$H^m=n$，于是 $H \subseteq G, n \in Z^*, Z>1.$

又 $n \mid p^m$，

$\therefore n=p^i\ (i=1,2,\cdots,m)$

令 $H_1=(a^{p^{i-1}})$，则 $H_1=(a^{p^{i-1}})$ 即为所求.

2. 设$f(x)=x^2+x+1$，（1）证明：商环$F_2[x]/(p(x))$构成域；（2）写出此有限域的乘法表（域元素用多项式形式表示）。（3）证明该域的乘法群为循环群。

证明：

显然有$x \nmid f(x), x+1 \nmid f(x)$，因此$f(x)$为$F_2[x]$中的不可约多项式，故$F_2[x]/(p(x))$构成域。

其次，乘法群的阶为3,即为素数，素数阶的群为循环群。

有限域$F_2[x]/(p(x))$的乘法表如下：

$\otimes$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	0	$x+1$	1	x

三、应用题（每小题20分，共20分）

1. 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$ed=1 \mod \varphi(n)$,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$n=143, e=103$。问：（1）若待加密的明文$M=113$， 求相应的密文C；（2）若待解密的密文$C=141$，求相应的明文M。

解：

（1）

密文$C = M^e \mod n = 113^{103} \mod 143 = 126$;

方法一：用反复平方法计算，$103 = (1100111)_2$

$$(1)\ n_0 = 1,\ a_0 = 113,\ b_1 = 113^2 = 42$$

$$(2)\ n_1 = 1,\ a_1 = a_0 \times b_1 = 27,\ b_2 = b_1^2 = 48$$

$$(3)\ n_2 = 1,\ a_2 = a_1 \times b_2 = 9,\ b_3 = b_2^2 = 16$$

$$(4)\ n_3 = 0,\ a_3 = a_2 = 9,\ b_4 = b_3^2 = 113$$

$$(5)\ n_4 = 0,\ a_4 = a_3 = 9,\ b_5 = b_4^2 = 42$$

$$(6)\ n_5 = 1,\ a_5 = a_4 \times b_5 = 92,\ b_6 = b_5^2 = 48$$

$$(7)\ n_6 = 1,\ a_6 = a_5 \times b_6 = 126$$

方法二：CRT

$$\begin{cases} x = 113^{103} = 5 \mod 11 \\ x = 113^{103} = 9 \mod 13 \end{cases}$$

$$x = 113^{103} \mod 143 = 5 \times 13 \times 6 + 5 \times 11 \times 6 = 126$$

（2）

首先用广义欧几里得算法求出私钥 $d = 7$;

则相应的明文 $M = C^d \mod n = 141^7 \mod 143 = (-2)^7 = -128 = 15$。