2.5元 (一) 信息安全数学基础

上海交通大学试卷（A卷）

（2011至2012学年 第2学期）

班级号 _____ 学号 _____ 姓名 _____

课程名称 信息安全数学基础（I） 成绩 _____

一. (15分)

i) 判断 $p = 151$ 是否为素数？

ii) 简述如何快速产生大素数

二. (15分) 设 $a = 179,\ b = 47.$

i) 求 $\frac{a}{b}$ 的连分数展开式.

ii) 求整数 $s,\ t$, 使得 $sp + tq = 1$

iii) 求解同余式组有解：

$$\begin{cases} x \equiv b_1 \pmod{179} \\ x \equiv b_2 \pmod{47} \end{cases}$$

三. (15分)

i) 设 a, b 是整数. 证明： a, b 互素 (即 $(a, b) = 1$) 的充要条件是存在整数 s, t 使得 $sa + tb = 1.$

ii) 设 p 是素数， a, b 是整数. 证明：当 $p \mid a \cdot b$ 时，有 $p \mid a$ 或 $p \mid b.$

我承诺，我将严格遵守考试纪律.

承诺人：_____

题 号										
得 分										
批阅人 (流水阅卷教师签名处)										

四. (15 分)

i) 判断同余式 $x^2 = 3 \bmod 179 \cdot 47$ 是否有解？

ii) 求解同余式 $x^2 = 3 \bmod 179 \cdot 47$.

五. (20 分) 叙述和证明欧拉定理.

六. (20 分)

i) 设 p 是素数. 对于整数 a, $p \nmid a$, 证明

序列 $\{a_k = a^k \mod p\}$ 是周期序列.

ii) 设 $\{a_k = a^k \mod p\}$ 的最小周期为 $p(a)$. 证明： $p(a) \mid p-1$.

iii) 求模 $p = 151$ 原根.

上 海 交 通 大 学 试 卷（B 卷）

（2011 至 2012 学年 第 2 学期）

班级号 _____ 学号 _____ 姓名 _____

课程名称 信息安全数学基础（I） 成绩 _____

一. (15 分)

i) 判断 $p = 157$ 是否为素数？

ii) 简述如何快速产生大素数

二. (15 分) 设 $a = 167,\ b = 59.$

i) 求 $\frac{a}{b}$ 的连分数展开式.

ii) 求整数 $s,\ t$, 使得 $sp + tq = 1$

iii) 求解同余式组有解：

$$\begin{cases} x \equiv b_1 \pmod{167} \\ x \equiv b_2 \pmod{59} \end{cases}$$

三. (15 分)

i) 设 a, b 是整数. 证明： a, b 互素 (即 $(a, b) = 1$) 的充要条件是存在整数 s, t 使得 $sa + tb = 1$.

ii) 设 p 是素数， a, b 是整数. 证明：当 $p \mid a \cdot b$ 时，有 $p \mid a$ 或 $p \mid b$.

我承诺，我将严格遵守考试纪律.

承诺人：_____

题 号										
得 分										
批阅人 (流水阅卷教师签名处)										

四. (15 分)

i) 判断同余式 $x^2 = 3 \bmod 167 \cdot 59$ 是否有解？

ii) 求解同余式 $x^2 = 3 \bmod 167 \cdot 59$.

五. (20 分) 叙述和证明欧拉定理.

六. (20 分)

i) 设 p 是素数. 对于整数 a, $p \nmid a$, 证明

序列 $\{a_k = a^k \mod p\}$ 是周期序列.

ii) 设 $\{a_k = a^k \mod p\}$ 的最小周期为 $p(a)$. 证明： $p(a) \mid p-1$.

iii) 求模 $p = 151$ 原根.

上 海 交 通 大 学 试 卷（A卷）
（2011至2012学年 第2学期）

一. (15分)

i) 判断 $p=151$ 是否为素数？

ii) 简述如何快速产生大素数

解 i) 因为 $\leq \sqrt{151} < 13$ 的所有素数为 2, 3, 5, 7, 11, 所以依次用 2, 3, 5, 7, 11, 13, 17 去试除.

$$151 = 75\cdot 2+1, \quad 151 = 50\cdot 3+1, \quad 151 = 30\cdot 5+1, \quad 151 = 21\cdot 7+4,$$
$$151 = 13\cdot 11+8.$$

所以 $N=151$ 为素数.

ii) 运用素性检验方法来快速产生大素数.

二. (15分) 设 $a=179$, $b=47$.

i) 求 $\frac{a}{b}$ 的连分数展开式.

ii) 求整数 s, t, 使得 $sp+tq=1$ (此处 $p=a$, $q=b$)

iii) 求解同余式组有解:

$$\begin{cases} x \equiv b_1 \pmod{179} \\ x \equiv b_2 \pmod{47} \end{cases}$$

解 设 $u_{-2}=a=179$, $u_{-1}=b=47$. 我们作广义欧几里得除法

$$\begin{array}{lrcrcll} \text{(i)} & 179 & = & 3\cdot 47 & + & 38, & 0<38=x_0\cdot 47<47. \\ \text{(ii)} & 47 & = & 1\cdot 38 & + & 9, & 0<9=x_1\cdot 38<38. \\ \text{(iii)} & 38 & = & 4\cdot 9 & + & 2, & 0<2=x_2\cdot 9<9. \\ \text{(iv)} & 9 & = & 4\cdot 2 & + & 1, & 0<1=x_3\cdot 2<2. \\ \text{(v)} & 2 & = & 2\cdot 1 & + & 0, & 0=x_4\cdot 1<1. \end{array}$$

i) 根据简单连分数的构造，我们有

(i) $a_0=[179/47]=3$, $\quad x_0=x-a_0=38/47$.

(ii) $a_1=[47/38]=1$, $\quad x_1=1/x_0-a_1=9/38$.

(iii) $a_2=[38/9]=4$, $\quad x_2=1/x_1-a_2=2/9$.

(iv) $a_3=[9/2]=4$, $\quad x_3=1/x_2-a_3=1/2$.

(v) $a_4=[2/1]=2$, $\quad x_4=1/x_3-a_4=0$.

因此, $\frac{a}{b}=[3,1,4,4,2]$.

ii) 由广义欧几里得除法，或由渐近连分数，得到

$$
\begin{aligned}
1 &= (-4)\cdot 2 &&+ 9\\
&= (-4)\cdot((-4)\cdot 9+38) &&+ 9\\
&= 17\cdot((-1)\cdot 38+47) &&+ (-4)\cdot 38\\
&= (-21)\cdot((-3)\cdot 47+179) &&+ 17\cdot 47\\
&= (-21)\cdot 179 &&+ 80\cdot 47
\end{aligned}
$$

i	a_i	x_i	P_i	Q_i
-2			0	1
-1			1	0
0	3	38/47	3	1
1	1	9/38	4	1
2	4	2/9	19	5
3	4	1/2	80	21
4	2	0	179	47

得到 $s=-21,\ t=80$.

iii) 根据中国剩余定理，取 $m_1=179, m_2=47$, 得到

$m=m_1\cdot m_2,\ \ , M_1=m/m_1=47,\ \ M_2=m/m_2=179,$

以及

$M_1'=(M_1)^{-1} \mod m_1=t=80,\ \ M_2'=(M_2)^{-1} \mod m_2=s=-21=26,$

从而，有一般解

$x\equiv M_1'\cdot M_1\cdot b_1+M_2'\cdot M_2\cdot b_2 \mod m.$

三. (15 分)

i) 设 a,b 是整数. 证明： a,b 互素 (即 $(a,b)=1$) 的充要条件
是存在整数 s,t 使得 $sa+tb=1$.

ii) 设 p 是素数， a,b 是整数. 证明：当 $p\mid a\cdot b$ 时，有
$p\mid a$ 或 $p\mid b$.

解 i) 必要性. 由广义欧几里得除法，存在整数 $s,\ t$ 使得 $sa+tb=(a,b)=1$.

充分性. 令 $d=(a,b)$. 由 $d|a,\ d|b$, 推得 $d|sa+tb=1$, 故 $d=1$.

ii)[证明一] 反证法. 若 $p\not|a$, 则 $(a,p)=1$. 由广义欧几里得除法，存在整数 $s,\ t$ 使得 $sa+tp=1$.

两端右乘 b, 得到 $s(ab)+(tb)p=b$. 推得 $p|s(ab)+(tb)p=b$.

[证明二] 反证法. 若 $p\not|a,\ p\not|a$, 则 $(a,p)=1,\ (b,p)=1$. 由 i) 存在整数 $s_1,\ t_1$ 及 $s_2,\ t_2$ ，使得 $s_1a+t_1p=1$ 及 $s_2b+t_2p=1$.

两式向乘，得到

$$s_1s_2(ab)+(s_1at_2+s_2bt_1+t_1t_2p)p=1.$$

推得 $(ab,p)=1$. 这与 $p\mid a\cdot b$ 矛盾.

四. (15 分)

i) 判断同余式 $x^2=3 \mod 179\cdot 47$ 是否有解？

ii) 求解同余式 $x^2=3 \mod 179\cdot 47$.

解 原同余式等价于同余式组

$$
\begin{cases}
x^2 &= 3 \mod 179\\
x^2 &= 3 \mod 47
\end{cases}
$$

计算勒让得符号

$$\left(\frac{3}{179}\right)=(-1)^{\frac{3-1}{2}\frac{179-1}{2}}\left(\frac{179}{3}\right)=(-1)\left(\frac{2}{3}\right)=(-1)(-1)^{(3^2-1)/8}=1,$$

$$\left(\frac{3}{47}\right)=(-1)^{\frac{3-1}{2}\frac{47-1}{2}}\left(\frac{47}{3}\right)=(-1)\left(\frac{-1}{3}\right)=(-1)(-1)^{(3-1)/8}=1,$$

故同余式组有解.

ii) 因为 $179\equiv 47\equiv 3 \bmod 4$, 所以原同余式的解为 (利用中国剩余定理)

$$x=(47^{-1} \bmod 179)\cdot 47\cdot(\pm 3^{(179+1)/4} \bmod 179)+(179^{-1} \bmod 47)\cdot 179\cdot(\pm 3^{(47+1)/4} \bmod 47)$$

五. (20 分) 叙述和证明欧拉定理.

解 欧拉定理是: 设 m 是大于 1 的整数. 如果 a 是满足 $(a,m)=1$ 的整数, 则

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

定理之证明 取 $r_1,\ \ldots,\ r_{\varphi(m)}$ 为模 m 的一个最小正简化剩余系, 则当 a 是满足 $(a,m)=1$ 的整数时, 根据 §2.3 定理 3 $ar_1,\ \ldots,\ ar_{\varphi(m)}$ 也为模 m 的一个简化剩余系, 这就是说, $ar_1,\ \ldots,\ ar_{\varphi(m)}$ 模 m 的最小正剩余是 $r_1,\ \ldots,\ r_{\varphi(m)}$ 的一个排列. 故乘积 $(ar_1)\cdots(ar_{\varphi(m)})$ 模 m 的最小正剩余和乘积 $r_1\cdots r_{\varphi(m)}$ 模 m 的最小正剩余相等. 根据 §2.1 定理 3 , 我们有

$$(ar_1)\cdots(ar_{\varphi(m)})\equiv r_1\cdots r_{\varphi(m)} \pmod m.$$

因此, $r_1\cdots r_{\varphi(m)}\ (a^{\varphi(m)}-1)\equiv 0 \pmod m$.

又从 $(r_1,m)=1,\ \ldots,\ (r_{\varphi(m)},m)=1$ 及 §1.4 定理 3, 可推出 $(r_1\cdots r_{\varphi(m)},\ m)=1$. 从而, 根据 §2.1 定理 8, 得到

$$a^{\varphi(m)}-1\equiv 0 \pmod m.$$

六. (20 分)

i) 设 p 是素数. 对于整数 a, $p\nmid a$, 证明

序列 $\{a_k=a^k \bmod p\}$ 是周期序列.

ii) 设 $\{a_k=a^k \bmod p\}$ 的最小周期为 $p(a)$. 证明: $p(a)\mid p-1$.

iii) 求模 $p=151$ 原根.

证 i) [证一] 因为 $a^k \bmod p\in\{1,\ldots,p-1\}$, 所以存在 $k,\ l$ 使得 $a^k\equiv a^l \bmod p$. 不妨设 $k>l$, 因为 $p\nmid p,\ (a,p)=1$, 所以 $a^{k-l}\equiv 1 \bmod p$. 故序列 $\{a_k=a^k \bmod p\}$ 是周期序列.

[证二] 由欧拉定理, 有 $a^{p-1}\equiv 1 \bmod p$, 所以对任意整数 k, 有 $a^{k+p-1}\equiv a^k \bmod p$. 故序列 $\{a_k=a^k \bmod p\}$ 是周期序列.

ii) 反证法. 若 $p(a)\nmid p-1$, 则存在整数 q,r 使得 $p-1=q\cdot p(a)+r,\quad 0\le r<p(a)$, 从而 $a^r\equiv a^r(a^{p-1})^q\equiv a^{p-1}\equiv 1 \bmod p$. 这与 $p(a)$ 的最小性矛盾.

iii) 设 $m=151$, 则 $\varphi(m)=\varphi(151)=2\cdot 3\cdot 5^2,\quad q_1=2,\ q_2=3,\ q_3=5$.

因此, $\varphi(m)/q_1=75,\quad \varphi(m)/q_2=50,\quad \varphi(m)/q_3=30$.

这样，只需验证： g^{75}, g^{50}, g^{30} 模 m 是否同余于 1. 对 2, 3, ... 逐个验算：

$$
\begin{array}{lllll}
2^2 \equiv 4, & 2^4 \equiv 16, & 2^5 \equiv 32, & 2^{10} \equiv 118, & \\
2^{20} \equiv 32, & 2^{25} \equiv 118, & 2^{30} \equiv 1, & 2^{50} \equiv 32, & 2^{75} \equiv 1, \\
3^2 \equiv 9, & 3^4 \equiv 81, & 3^5 \equiv 92, & 3^{10} \equiv 8, & \\
3^{20} \equiv 64, & 3^{25} \equiv 150, & 3^{30} \equiv 59, & 3^{50} \equiv 1, & 3^{75} \equiv 150, \\
5^2 \equiv 25, & 5^4 \equiv 21, & 5^5 \equiv 105, & 5^{10} \equiv 2, & \\
5^{20} \equiv 4, & 5^{25} \equiv 118, & 5^{30} \equiv 8, & 5^{50} \equiv 32, & 5^{75} \equiv 1, \\
6^2 \equiv 36, & 6^4 \equiv 88, & 6^5 \equiv 75, & 6^{10} \equiv 38, & \\
6^{20} \equiv 85, & 6^{25} \equiv 33, & 6^{30} \equiv 59, & 6^{50} \equiv 32, & 2^{75} \equiv 150, \\
7^2 \equiv 49, & 7^4 \equiv 136, & 7^5 \equiv 46, & 7^{10} \equiv 2, & \\
7^{20} \equiv 4, & 7^{25} \equiv 33, & 7^{30} \equiv 8, & 7^{50} \equiv 32, & 7^{75} \equiv 150, \\
\multicolumn{5}{l}{(\mathrm{mod}\ 151).}
\end{array}
$$

因此， $g = 6, 7$ 是模 151 的原根.

当 d 遍历模 $\varphi(m) = 150 = 2 \cdot 3 \cdot 5^2$ 的简化剩余系时， g^d 遍历模 p 的所有原根.

上 海 交 通 大 学 试 卷（B卷）

（2011至2012学年 第2学期）

一. (15分)

i) 判断 $p=157$ 是否为素数？

ii) 简述如何快速产生大素数

解 i) 因为 $\leq \sqrt{157} < 13$ 的所有素数为 2, 3, 5, 7, 11, 所以依次用 2, 3, 5, 7, 11, 13, 17 去试除.

$$157 = 78\cdot 2+1, \quad 157 = 52\cdot 3+1, \quad 157 = 31\cdot 5+2, \quad 157 = 22\cdot 7+3,$$
$$157 = 14\cdot 11+3.$$

所以 $N=157$ 为素数.

ii) 运用素性检验方法来快速产生大素数.

二. (15分) 设 $a=167$, $b=59$.

i) 求 $\frac{a}{b}$ 的连分数展开式.

ii) 求整数 s, t, 使得 $sp+tq=1$

iii) 求解同余式组有解:

$$\begin{cases} x \equiv b_1 \pmod{167} \\ x \equiv b_2 \pmod{59} \end{cases}$$

解 设 $u_{-2}=a=167$, $u_{-1}=b=59$. 我们作广义欧几里得除法

$$\begin{array}{lrcl} \text{(i)} & 167 & = 2\cdot 59 + 49, & 0<49=x_0\cdot 59<59. \\ \text{(ii)} & 59 & = 1\cdot 49 + 10, & 0<10=x_1\cdot 49<49. \\ \text{(iii)} & 49 & = 4\cdot 10 + 9, & 0<9=x_2\cdot 10<10. \\ \text{(iv)} & 10 & = 1\cdot 9 + 1, & 0<1=x_3\cdot 9<9. \\ \text{(v)} & 9 & = 9\cdot 1 + 0, & 0=x_4\cdot 1<1. \end{array}$$

i) 根据简单连分数的构造，我们有

(i) $a_0=[167/59]=2$, $x_0=x-a_0=49/59$.

(ii) $a_1=[59/49]=1$, $x_1=1/x_0-a_1=10/49$.

(iii) $a_2=[49/10]=4$, $x_2=1/x_1-a_2=9/10$.

(iv) $a_3=[10/9]=1$, $x_3=1/x_2-a_3=1/9$.

(v) $a_4=[9/1]=9$, $x_4=1/x_3-a_4=0$.

因此, $\frac{a}{b}=[2,1,4,1,9]$.

ii) 由广义欧几里得除法，或由渐近连分数，得到

$$
\begin{aligned}
1 &= (-1)\cdot 9 &&+ 10\\
&= (-1)\cdot((-4)\cdot 10+49) &&+ 10\\
&= 5\cdot((-1)\cdot 49+59) &&+ (-1)\cdot 49\\
&= (-6)\cdot((-2)\cdot 59+167) &&+ 5\cdot 59\\
&= (-6)\cdot 167 &&+ 17\cdot 59
\end{aligned}
$$

i	a_i	x_i	P_i	Q_i
-2			0	1
-1			1	0
0	2	49/59	2	1
1	1	10/49	3	1
2	4	9/10	14	5
3	1	1/9	17	6
4	9	0	167	59

得到 $s=-6,\ t=17$.

iii) 根据中国剩余定理，取 $m_1=167, m_2=59$, 得到

$m=m_1\cdot m_2,\ \ , M_1=m/m_1=59,\ \ M_2=m/m_2=167,$

以及

$M_1'=(M_1)^{-1} \mod m_1=t=17,\ \ M_2'=(M_2)^{-1} \mod m_2=s=-6=53,$

从而，有一般解

$x\equiv M_1'\cdot M_1\cdot b_1+M_2'\cdot M_2\cdot b_2 \mod m.$

三. (15 分)

i) 设 a,b 是整数. 证明： a,b 互素 (即 $(a,b)=1$) 的充要条件
是存在整数 s,t 使得 $sa+tb=1$.

ii) 设 p 是素数， a,b 是整数. 证明：当 $p\mid a\cdot b$ 时，有
$p\mid a$ 或 $p\mid b$.

解 i) 必要性. 由广义欧几里得除法，存在整数 $s,\ t$ 使得 $sa+tb=(a,b)=1$.

充分性. 令 $d=(a,b)$. 由 $d|a,\ d|b$, 推得 $d|sa+tb=1$, 故 $d=1$.

ii)[证明一] 反证法. 若 $p\not|a$, 则 $(a,p)=1$. 由广义欧几里得除法，存在整数 $s,\ t$ 使得 $sa+tp=1$.

两端右乘 b, 得到 $s(ab)+(tb)p=b$. 推得 $p|s(ab)+(tb)p=b$.

[证明二] 反证法. 若 $p\not|a,\ p\not|a$, 则 $(a,p)=1,\ (b,p)=1$. 由 i) 存在整数 $s_1,\ t_1$ 及 $s_2,\ t_2$, 使得 $s_1a+t_1p=1$ 及 $s_2b+t_2p=1$.

两式向乘，得到

$$s_1s_2(ab)+(s_1at_2+s_2bt_1+t_1t_2p)p=1.$$

推得 $(ab,p)=1$. 这与 $p\mid a\cdot b$ 矛盾.

四. (15 分)

i) 判断同余式 $x^2=3 \mod 167\cdot 59$ 是否有解？

ii) 求解同余式 $x^2=3 \mod 167\cdot 59$.

解 原同余式等价于同余式组

$$
\begin{cases}
x^2 &= 3 \mod 167\\
x^2 &= 3 \mod 59
\end{cases}
$$

计算勒让得符号

$$\left(\frac{3}{167}\right)=(-1)^{\frac{3-1}{2}\frac{167-1}{2}}\left(\frac{167}{3}\right)=(-1)\left(\frac{2}{3}\right)=(-1)(-1)^{(3^2-1)/8}=1,$$

$$\left(\frac{3}{59}\right)=(-1)^{\frac{3-1}{2}\frac{59-1}{2}}\left(\frac{59}{3}\right)=(-1)\left(\frac{-1}{3}\right)=(-1)(-1)^{(3-1)/8}=1,$$

故同余式组有解.

ii) 因为 $167\equiv 59\equiv 3 \bmod 4$, 所以原同余式的解为 (利用中国剩余定理)

$$x=(59^{-1} \bmod 167)\cdot 59\cdot(\pm 3^{(167+1)/4} \bmod 167)+(167^{-1} \bmod 59)\cdot 167\cdot(\pm 3^{(59+1)/4} \bmod 59)$$

五. (20 分) 叙述和证明欧拉定理.

解 欧拉定理是: 设 m 是大于 1 的整数. 如果 a 是满足 $(a,m)=1$ 的整数, 则

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

定理之证明 取 $r_1,\ \ldots,\ r_{\varphi(m)}$ 为模 m 的一个最小正简化剩余系, 则当 a 是满足 $(a,m)=1$ 的整数时, 根据 §2.3 定理 3 $ar_1,\ \ldots,\ ar_{\varphi(m)}$ 也为模 m 的一个简化剩余系, 这就是说, $ar_1,\ \ldots,\ ar_{\varphi(m)}$ 模 m 的最小正剩余是 $r_1,\ \ldots,\ r_{\varphi(m)}$ 的一个排列. 故乘积 $(ar_1)\cdots(ar_{\varphi(m)})$ 模 m 的最小正剩余和乘积 $r_1\cdots r_{\varphi(m)}$ 模 m 的最小正剩余相等. 根据 §2.1 定理 3 , 我们有

$$(ar_1)\cdots(ar_{\varphi(m)})\equiv r_1\cdots r_{\varphi(m)} \pmod m.$$

因此, $r_1\cdots r_{\varphi(m)}\ (a^{\varphi(m)}-1)\equiv 0 \pmod m$.

又从 $(r_1,m)=1,\ \ldots,\ (r_{\varphi(m)},m)=1$ 及 §1.4 定理 3, 可推出 $(r_1\cdots r_{\varphi(m)},\ m)=1$. 从而, 根据 §2.1 定理 8, 得到

$$a^{\varphi(m)}-1\equiv 0 \pmod m.$$

六. (20 分)

i) 设 p 是素数. 对于整数 a, $p\nmid a$, 证明

序列 $\{a_k=a^k \bmod p\}$ 是周期序列.

ii) 设 $\{a_k=a^k \bmod p\}$ 的最小周期为 $p(a)$. 证明: $p(a)\mid p-1$.

iii) 求模 $p=151$ 原根.

证 i) [证一] 因为 $a^k \bmod p\in\{1,\ldots,p-1\}$, 所以存在 $k,\ l$ 使得 $a^k\equiv a^l \bmod p$. 不妨设 $k>l$, 因为 $p\nmid p$, $(a,p)=1$, 所以 $a^{k-l}\equiv 1 \bmod p$. 故序列 $\{a_k=a^k \bmod p\}$ 是周期序列.

[证二] 由欧拉定理, 有 $a^{p-1}\equiv 1 \bmod p$, 所以对任意整数 k, 有 $a^{k+p-1}\equiv a^k \bmod p$. 故序列 $\{a_k=a^k \bmod p\}$ 是周期序列.

ii) 反证法. 若 $p(a)\nmid p-1$, 则存在整数 q,r 使得 $p-1=q\cdot p(a)+r,\quad 0\le r<p(a)$, 从而 $a^r\equiv a^r(a^{p-1})^q\equiv a^{p-1}\equiv 1 \bmod p$. 这与 $p(a)$ 的最小性矛盾.

iii) 设 $m=151$, 则 $\varphi(m)=\varphi(151)=2\cdot 3\cdot 5^2,\quad q_1=2,\ q_2=3,\ q_3=5$.

因此, $\varphi(m)/q_1=75,\quad \varphi(m)/q_2=50,\quad \varphi(m)/q_3=30$.

这样，只需验证： g^{75}, g^{50}, g^{30} 模 m 是否同余于 1. 对 2, 3, ... 逐个验算：

$$
\begin{array}{lllll}
2^2 \equiv 4, & 2^4 \equiv 16, & 2^5 \equiv 32, & 2^{10} \equiv 118, & \\
2^{20} \equiv 32, & 2^{25} \equiv 118, & 2^{30} \equiv 1, & 2^{50} \equiv 32, & 2^{75} \equiv 1, \\
3^2 \equiv 9, & 3^4 \equiv 81, & 3^5 \equiv 92, & 3^{10} \equiv 8, & \\
3^{20} \equiv 64, & 3^{25} \equiv 150, & 3^{30} \equiv 59, & 3^{50} \equiv 1, & 3^{75} \equiv 150, \\
5^2 \equiv 25, & 5^4 \equiv 21, & 5^5 \equiv 105, & 5^{10} \equiv 2, & \\
5^{20} \equiv 4, & 5^{25} \equiv 118, & 5^{30} \equiv 8, & 5^{50} \equiv 32, & 5^{75} \equiv 1, \\
6^2 \equiv 36, & 6^4 \equiv 88, & 6^5 \equiv 75, & 6^{10} \equiv 38, & \\
6^{20} \equiv 85, & 6^{25} \equiv 33, & 6^{30} \equiv 59, & 6^{50} \equiv 32, & 2^{75} \equiv 150, \\
7^2 \equiv 49, & 7^4 \equiv 136, & 7^5 \equiv 46, & 7^{10} \equiv 2, & \\
7^{20} \equiv 4, & 7^{25} \equiv 33, & 7^{30} \equiv 8, & 7^{50} \equiv 32, & 7^{75} \equiv 150, \\
\multicolumn{5}{l}{(\mathrm{mod}\ 151).}
\end{array}
$$

因此， $g = 6, 7$ 是模 151 的原根.

当 d 遍历模 $\varphi(m) = 150 = 2 \cdot 3 \cdot 5^2$ 的简化剩余系时， g^d 遍历模 p 的所有原根.

上 海 交 通 大 学 试 卷（A卷）

（2008至2009学年 第1学期）

班级号 _____ 学号 _____ 姓名 _____

课程名称 信息安全数学基础（I） 成绩 _____

一. (20分)

i) 判断359是否为素数？

ii) 简述如何快速产生大素数

二. (20分) 设 $a = 359,\ b = 47.$

i) 求 $\frac{a}{b}$ 的连分数展开式.

ii) 求整数 $s,\ t$, 使得 $sp + tq = 1$

三. (20 分) 设 $m_1, \ldots, m_k$ 是互素的正整数. 证明下列同余式组有解:

i)
$$\begin{cases} x \equiv b_1 \pmod{m_1} \\ x \equiv 0 \pmod{m_2} \\ \quad \vdots \\ x \equiv 0 \pmod{m_k} \end{cases}$$

ii) 对于 $2 \le i \le k$,
$$\begin{cases} x \equiv 0 \pmod{m_1} \\ \quad \vdots \\ x \equiv 0 \pmod{m_{i-1}} \\ x \equiv b_i \pmod{m_i} \\ x \equiv 0 \pmod{m_{i+1}} \\ \quad \vdots \\ x \equiv 0 \pmod{m_k} \end{cases}$$

iii)
$$\begin{cases} x \equiv b_1 \pmod{m_1} \\ \quad \vdots \\ x \equiv b_k \pmod{m_k} \end{cases}$$

我承诺，我将严格遵守考试纪律.

承诺人：_____

题号										
得分										
批阅人 (流水阅卷教师签名处)										

四. (20 分)

i) 判断同余式 $x^2 = 47 \bmod 359$ 是否有解.

ii) 简述模重复平方法

ii) 求解同余式 $x^2 = 47 \bmod 359$.

五. (20 分)

i) 简述欧拉定理.

ii) 求模 $p = 359$ 原根.

iii) 设 $p = 359$. 对所有因数 $d|p-1$, 求相应的整数 a , 使得 $\mathrm{ord}_p(a) = d$.

上海交通大学试卷（B卷）
（2008至2009学年 第1学期）

班级号 _____ 学号 _____ 姓名 _____

课程名称 信息安全数学基础（I） 成绩 _____

一. (20分)

i) 判断383是否为素数？

ii) 简述如何快速产生大素数

二. (20分) 设 $a = 383,\ b = 43.$

i) 求 $\frac{a}{b}$ 的连分数展开式.

ii) 求整数 $s,\ t$, 使得 $sp + tq = 1$

三. (20 分) 设 $m_1, \ldots, m_k$ 是互素的正整数. 证明下列同余式组有解:

i)
$$\begin{cases} x \equiv b_1 \pmod{m_1} \\ x \equiv 0 \pmod{m_2} \\ \quad \vdots \\ x \equiv 0 \pmod{m_k} \end{cases}$$

ii) 对于 $2 \le i \le k$,
$$\begin{cases} x \equiv 0 \pmod{m_1} \\ \quad \vdots \\ x \equiv 0 \pmod{m_{i-1}} \\ x \equiv b_i \pmod{m_i} \\ x \equiv 0 \pmod{m_{i+1}} \\ \quad \vdots \\ x \equiv 0 \pmod{m_k} \end{cases}$$

iii)
$$\begin{cases} x \equiv b_1 \pmod{m_1} \\ \quad \vdots \\ x \equiv b_k \pmod{m_k} \end{cases}$$

我承诺，我将严格遵守考试纪律.

承诺人：_____

题 号										
得 分										
批阅人 (流水阅卷教师签名处)										

四. (20 分)

i) 判断同余式 $x^2 = 43 \bmod 383$ 是否有解.

ii) 简述模重复平方法

ii) 求解同余式 $x^2 = 43 \bmod 383$.

五. (20 分)

i) 简述欧拉定理.

ii) 求模 $p = 383$ 原根.

iii) 设 $p = 383$. 对所有因数 $d|p-1$, 求相应的整数 a , 使得 $\mathrm{ord}_p(a) = d$.

2.5