Research Inventy: International Journal Of Engineering And Science
Vol.3, Issue 7 (August2013), PP 43-58
Issn(e): 2278-4721, Issn(p):2319-6483, Www.Researchinventy.Com

Several problems in elementary number theory

Kaifu SONG[a],*

[a] East Lake High School, Yichang, Hubei, China.
East Lake High School, Yichang 443100, Hubei, China

ABSTRACT: We will give a character of indefinite equation and a solution of unitary congruence equation and quadratic congruence equation, reveal the relation among the original root of Odd prime Numbers, the Simplified residue system and Square residual.

Keywords: Pythagorean number; Unitary congruence equation; Quadratic congruence equation; The original root.

MR(2000)：08B10；1CLC: 0156.1.

I. PYTHAGOREAN NUMBER

Theorem 1. x、y、$z\in Z_+$ (Z is set of integers)，$x>2$，equation $x^2+y^2=z^2$ （Ⅰ), at least has a group of solution.

Proof. $x^2=z^2-y^2=(z+y)(z-y)$.

(i) when $x=2m+1$，$m\in Z_+$， m such that $(z+y)(z-y)=(2m+1)^2$ holds.

Set $z-y=1$，$z+y=(2m+1)^2$, we have $x=2m+1$，$y=2m^2+2m$, $z=2m^2+2m+1$.

(ii) when $x=2m$，and $m\geq 2$ ，m such that $(z+y)(z-y)=4m^2$holds.

Set $z-y=2$，$z+y=2m^2$，we have $x=2m$，$y=m^2-1$，$z=m^2+1$. □

Satisfied (Ⅰ) Three positive integers x, y and z are called *Pythagorean number*.

Example 1. Write Check Pythagorean number based on the following number.

（1）37， （2）40.

Answer:（1）Set $x=2m+1=37$，we have $m=18$．$y=2m^2+2m=684$，$z=y+1=685$.

Then $37^2+684^2=685^2$;

Set $z=2m^2+2m+1=37$，then $m\notin Z$；Set $y=m^2-1=37$，then $m\notin Z$;

Set $z=m^2+1=37$，we have $m=6$．$x=12$，$y=35$. Then$12^2+35^2=37^2$.

Therefore, we can have two groups of Check Pythagorean number.

（2）Set $x^2=(2m)^2=4m^2=1\times1600=2\times800=4\times400=5\times320=8\times200=10\times160=16\times100$
$=20\times80=25\times64=32\times50=40\times40$.

Set $z-y=2$，$z+y=2m^2=800$, we have $x=40$，$y=399$，$z=401$;

Set $z-y=4$，$z+y=2m^2=400$, we have $x=40$，$y=198$，$z=202$;

Set $z-y=8$，$z+y=2m^2=200$, we have $x=40$，$y=96$，$z=104$;

Set $z-y=10$，$z+y=2m^2=160$, we have $x=40$，$y=75$，$z=85$;

Set $z-y=16$，$z+y=2m^2=100$, we have $x=40$，$y=42$，$z=58$;

Set $z-y=20$，$z+y=2m^2=80$, we have $x=40$，$y=30$，$z=50$;

Set $z-y=32$，$z+y=2m^2=50$, we have $x=40$，$y=9$，$z=41$;

Set $z=m^2+1=5$，$m=2$，we have $4^2+3^2=5^2$，$32^2+24^2=40^2$. $x=32$，$y=24$，$z=40$.

Therefore, we can write 8 groups of Check Pythagorean number based on 40.

Theorem 2 x、y、z、$l\in Z_+$，equation $x^2+y^2+z^2=l^2$ at least has a group of solution.

Proof. $1^2+2^2+2^2=3^2$; $x>2$, by the theorem 1，

$x^2+y^2=z_1^2$，$z_1>2$. $z_1^2+z^2=l^2$. we have $x^2+y^2+z^2=l^2$. □

$x\geq 3$,

$$\begin{cases} x=2m+1 \\ y=2m^2+2m \\ z=\frac{1}{2}[(2m^2+2m+1)^2-1] \\ l=\frac{1}{2}[(2m^2+2m+1)^2+1]; \end{cases} \quad \begin{cases} x=2m(m \text{ is an even number}) \\ y=m^2-1 \\ z=\frac{1}{2}[(m^2+1)^2-1] \\ l=\frac{1}{2}[(m^2+1)^2+1]; \end{cases} \quad \begin{cases} x=2m(\ m \text{ is an odd number of}) \\ y=m^2-1 \\ z=\frac{1}{4}(m^2+1)^2-1 \\ l=\frac{1}{4}(m^2+1)^2+1. \end{cases}$$

Theorem 3 $x_i\in Z_+$, $n\geq 3$, equation $x_1^2+x_2^2+\cdots+x_n^2=x_{n+1}^2$ at least has a group of solution.

II. CONGRUENCE THEORY

Prove the theorem4using Congruence theory.

Theorem 4. If $a,b\in Z$, and not both are 0, Then there exist s x, $y\in Z$ such that $ax+by=(a, b)$ holds.

Proof. Form $ax+by=(a, b)$, we have $\frac{a}{(a,b)}x+\frac{b}{(a,b)}y=1$, mark $m=\frac{a}{(a,b)}$, $n=\frac{b}{(a,b)}$, then we have $mx+ny=1$.

Suppose that A is complete residue system of m, Since $(m, n)=1$, nA is also the complete residue system of m, then therenA exists na_i and 1 in A such that $na_i\equiv 1(\mathrm{mod}m)$holds. Take $y=a_i$, then $x=\frac{1-ny}{m}\in Z$.

□

III. ONE-PLACE CONGRUENT EQUATION SOLUTION

3.1. Prime Number Module of Higher Degree Congruence Equation

Lemma 1. (*J.L.Lagrange* theorem) $n(<p)$ congruence equation $f(x)\equiv 0(\mathrm{mod}p)$ $((p,a_n)=1)$ (Ⅱ), necessary and sufficient condition of n different solutions is: $x^p-x\equiv q(x)f(x)\ (\mathrm{mod}\ p)$.

Theorem 5. $n(<p)$congruence equation $f(x)\equiv 0(\mathrm{mod}p)$ (Ⅱ), necessary and sufficient condition of having a solution:

$f(x)=q(x)r(x)\equiv 0\ (\mathrm{mod}\ p)$, and $x^p-x=g(x)f(x)+r(x)\equiv 0(\mathrm{mod}p)$.

If the degree of $r(x)$ is m, (Ⅱ)has m different solutions. $m\leq n$.

Proof. $f(x)=q(x)r(x)\equiv 0\ (\mathrm{mod}\ p)$, $x^p-x=g(x)f(x)+r(x)\equiv r(x)[\ g(x)q(x)+1]\equiv 0\ (\mathrm{mod}\ p)$. By the lemma 1, $r(x)\equiv 0\ (\mathrm{mod}p)$ has m different solutions. So (Ⅱ) has m different solutions. Necessary is obvious. □

Example 2. Solve equation $f(x)\equiv 0\ (\mathrm{mod}\ 7)$.

$f(x)=2x^{17}+6x^{16}+x^{14}+5x^{12}+3x^{11}+2x^{10}+x^9+5x^8+2x^7+3x^5+4x^4+6x^3+4x^2+x+4$.

Answer: $f(0)\not\equiv 0(\mathrm{mod}\ 7)$, $f(x)\equiv(x^6-1)\ g_1(x)+r_1(x)\ (\mathrm{mod}\ 7)$.We have,

$g_1(x)=2x^{11}-x^{10}+x^8-2x^6-2x^5+x^4+x^3-x^2+2x-2$, $r_1(x)=x^5-2x^4+3x^2+3x+2$.

$x^6-1\equiv r_1(x)\ g_2(x)+r_2(x)\ (\mathrm{mod}\ 7)$. where, $g_2(x)=x+2$, $r_2(x)\equiv x^4+x^3+3x^2-2x-3(\mathrm{mod}\ 7)$.

$r_1(x)\equiv r_2(x)\ g_3(x)\ (\mathrm{mod}\ 7)$, so $r_3(x)\equiv 0\ (\mathrm{mod}\ 7)$.

The solution of $r_2(x)\equiv 0\ (\mathrm{mod}\ 7)$ is different with the solution of $f(x)\equiv 0\ (\mathrm{mod}\ 7)$.

$x^6-1\equiv(x^2-x-2)r_2(x)\ (\mathrm{mod}\ 7)$, the solution of $x^3-x^2-2x\equiv 0\ (\mathrm{mod}\ 7)$ is $x\equiv 0,\ -1,\ 2(\mathrm{mod}\ 7)$.

The different solutions of $f(x)\equiv 0\ (\mathrm{mod}\ 7)$ is complementary with the solution of $x^3-x^2-2x\equiv 0\ (\mathrm{mod}\ 7)$.

The different solutions of $f(x)\equiv 0\ (\mathrm{mod}\ 7)$ is $x\equiv 1,-2,\pm 3\ (\mathrm{mod}\ 7)$.

3.2. Equations $\begin{cases} x\equiv a(\mathrm{mod}m) \\ x\equiv b(\mathrm{mod}n) \end{cases}$ (Ⅲ), the necessary and sufficient conditions for solvability

Theorem 6. Equations $\begin{cases} x\equiv a(\mathrm{mod}m) \\ x\equiv b(\mathrm{mod}n) \end{cases}$ (Ⅲ), the necessary and sufficient conditions for solvability is: $a+mt\equiv b\ (\mathrm{mod}\ n)$ (or $b+nt\equiv a\ (\mathrm{mod}\ m)$), $t\in \boldsymbol{Z}$.

if so，the solution is (Ⅲ) $x\equiv a+mt(\mathrm{mod}[m, n])$ (or $x\equiv b+nt(\mathrm{mod}[m, n])$).

Proof. $x\equiv b\equiv a+mt(\mathrm{mod}\ n)$，$x\equiv a+mt(\mathrm{mod}\ m)$. so $x\equiv a+mt(\mathrm{mod}[m, n])$.

$x\equiv a+mt(\mathrm{mod}[m, n])$，so $x\equiv a+mt(\mathrm{mod}\ n)$，and $x\equiv b(\mathrm{mod}\ n)$. so $a+mt\equiv b\ (\mathrm{mod}\ n)$. □

Theorem7. Equations $\begin{cases} x\equiv b_1\ (\mathrm{mod}m_1) \\ \cdots \\ x\equiv b_n\ (\mathrm{mod}m_n) \end{cases}$ (Ⅳ), the necessary and sufficient conditions for solvability is:$b_1+m_1t_1+[m_1,m_2]\ t_2+\cdots+[\ m_1，\ m_2，\ \cdots，\ m_i]\ t_i\equiv b_{i+1}(\mathrm{mod}m_{i+1})$，$i$=1,2,$\cdots$,$n$－1.

If so, the solution of (Ⅳ)is :$x\equiv b_1+m_1t_1+[m_1,m_2]\ t_2+\cdots+[\ m_1，\ m_2，\ \cdots，\ m_{n-1}]\ t_{n-1}(\mathrm{mod}[m_1，\ m_2,\cdots，\ m_n])$.

Proof. by the theorem 6，n=1,2 the proposition is true. If$n=k$ we suppose the proposition is true.

The solution of(Ⅳ) is: $x\equiv b_1+m_1t_1+[m_1,m_2]\ t_2+\ldots+[\ m_1, m_2,\ldots,m_{k-1}]\ t_{k-1}(\mathrm{mod}[m_1，\ m_2,\ldots,m_k])$.

t_{k-1} satisfy $b_1+m_1t_1+[m_1,m_2]\ t_2+\ldots+[\ m_1，\ m_2，\ \ldots，\ m_{k-1}]\ t_{k-1}\equiv b_k(\mathrm{mod}m_k)$.$n=k$+1, we have

$$\begin{cases} x\equiv b_{k+1}(\mathrm{mod}m_{k+1}) \\ x\equiv b_1+m_1t_1+[m_1,m_2]\ t_2+\ldots+[\ m_1，\ m_2，\ \ldots，\ m_{k-1}]\ t_{k-1}(\mathrm{mod}[m_1，\ m_2，\ \ldots，\ m_k]). \end{cases} \quad (\dagger)$$

By theorem 6，t_k the solution of $b_1+m_1t_1+[m_1,m_2]\ t_2+\ldots+[\ m_1，\ m_2，\ \ldots，\ m_i]\ t_i\equiv b_{i+1}(\mathrm{mod}m_{i+1})$. ($\dagger$)is the solution of (Ⅳ), then the solution of(Ⅳ)is :

$x\equiv b_1+m_1t_1+[m_1,m_2]\ t_2+\ldots+[\ m_1，\ m_2，\ \ldots，\ m_k]\ t_k\ (\mathrm{mod}[m_1，\ m_2，\ \ldots，\ m_{k+1}])$.

Then $n=k$+1, the proposition is true. □

Example 3. Solve the system $\begin{cases} x\equiv 1(\mathrm{mod}15) \\ x\equiv -2(\mathrm{mod}12) \\ x\equiv 6(\mathrm{mod}10) \end{cases}$.

Answer: 1+15 $t_1\equiv -2(\mathrm{mod}\ 12)$，$t_1=-1$；1+15 t_1+60 $t_2\equiv 6(\mathrm{mod}\ 10)$，$t_2=0$.

the solution for the system is $x\equiv 1-15\equiv -14\equiv 46\ (\mathrm{mod}\ 60)$.

3.3. Congruent equations group Mode expansion

$f(x)=\sum_{i=0}^{n} a_i x^{n-i}$，$a_i\in \boldsymbol{Z}$，$a_0\neq 0$，$(a_0, a_1, \ldots, a_n)=1$，$f(x)$ for the simplest polynomial with integer coefficients.

Theorem 8. For System $\begin{cases} f\equiv r_1\ (\mathrm{mod}m) \\ f\equiv r_2(\mathrm{mod}n) \end{cases}$ (Ⅴ)，it has solution when satisfy the necessary and sufficient condition:$mt+\ r_1\equiv r_2\ (\mathrm{mod}\ n)$ (or $nt+\ r_2\equiv r_1\ (\mathrm{mod}\ m)$).

The solution for system (V) is $f\equiv mk+\ r_1\equiv r_2\ (\mathrm{mod}[\mathrm{m}, n])$.

NOTICE: Here,f，r_1，r_2，t, m，n is the minimalist integral coefficient polynomial, $\partial^\circ r_1<\partial^\circ m$，$\partial^\circ r_2<\partial^\circ n(\partial^\circ f(x)$for the number of x).

Proof. set $f\equiv r_2\equiv mt+\ r_1\ (\mathrm{mod}\ n)$, $x\equiv mt+\ r_1\ (\mathrm{mod}\ m)$. such that: $f\equiv mt+\ r_1\ (\mathrm{mod}[m, n])$.

$f\equiv mt+\ r_1\ (\mathrm{mod}[m, n])$，such that $f\equiv mt+\ r_1\ (\mathrm{mod}\ n)$，$f\equiv r_2\ (\mathrm{mod}\ n)$. hen we have:$mt+\ r_1\equiv r_2\ (\mathrm{mod}\ n)$. □

Example 4. Solve the system $\begin{cases} f(x)\equiv r_1(\mathrm{mod}\ g_1(x)) & ① \\ f(x)\equiv r_2(\mathrm{mod}\ g_2(x)) & ②. \\ f(x)\equiv r_3(\mathrm{mod}\ g_3(x)) & ③ \end{cases}$

Here, $r_1(x)=13x^2-8x+26$, $g_1(x)=x^3+2x^2+3$; $r_2(x)=105x-60$, $g_2(x)=x^2-4x+2$; $r_3(x)=52$, $g_3(x)=x+2$.

Answer: Set $g_1(x)\ p(x)+\ r_1(x)\equiv r_2(\mathrm{mod}\ g_2(x))$, it is $(22x-9)\ p(x)-61x+60\equiv 0(\mathrm{mod}\ g_2(x))$, then we have: $-61x+60\not\equiv 0(\mathrm{mod}\ g_2(x))$, $\partial^\circ(22x-9)=1, \partial^\circ(g_2(x))=2$.

Set $p(x)=ax+b$, we have :$(22x-9)(ax+b)-61x+60\equiv 22ax^2-(9a-22b+61)x-(9b-60)\equiv c(x^2-4x+2)(\mathrm{mod}\ g_2(x))$, because $22a=c$, $9a-22b+61=4c$, $9b-60=-2c$, then we have $a=3$, $b=-8$, therefore $p(x)=3x-8$.

So the solution for equations ①&② is $f(x)\equiv g_1(x)\ p(x)+\ r_1(x)\equiv 3\ x^4-2\ x^3-3\ x^2+\ x+2(\mathrm{mod}\ g_1(x)g_2(x))$,

because $3x^4-2x^3-3x^2+x+2\equiv 52 \pmod{g_3(x)}$, the solution for the system is $f(x)\equiv 3x^4-2x^3-3x^2+x+2 \pmod{g_1(x)g_2(x)g_3(x)}$.

IV. THE SOLUTION OF QUADRATIC CONGRUENCE EQUATION

4.1. The solution of quadratic congruence equation for a odd prime module

Theorem 9. p is a prime number, for equations, $x^2\equiv b \pmod p$ (VI), $x\equiv\pm\frac{p-1}{2} \pmod p$ (VII),

(VII) is the a solution of (VI) , here: $p=4n+1$, $b=-\frac{p-1}{4}$; $p=4n+3$, $b=\frac{p+1}{4}$.

Proof. (i) $p=4n+1$, $x^2-b\equiv\frac{(p-1)^2}{4}+\frac{p-1}{4}\equiv\frac{p(p-1)}{4}\equiv 0 \pmod p$;

(ii) $p=4n+3$, $x^2-b\equiv\frac{(p-1)^2}{4}-\frac{p+1}{4}\equiv\frac{p(p-3)}{4}\equiv 0 \pmod p$.

From Lemma 1, (Ⅶ) is the solution of (Ⅵ). □

Definition 1. p is a prime number, then $x^2\equiv b \pmod p$ is called $x\equiv\pm\frac{p-1}{2} \pmod p$ *benchmark equation*.

Theorem 10. p is a prime number, $(p, a)=1$, $x^2\equiv a \pmod p$. (Ⅷ)

(i) $a\equiv b \pmod p$, the solution of (Ⅷ) is $x\equiv\pm\frac{p-1}{2} \pmod p$;

(ii) $a\not\equiv b \pmod p$, the necessary and sufficient condition for euqtion (Ⅷ) has solution is $m(m+1)\equiv a-b \pmod p$. $m=1,2,\text{---},n-1$.

If that, the solution for equation (Ⅷ) is $x\equiv\pm(\frac{p-1}{2}-m) \pmod p$, when $p=4n+1$, $b=-\frac{p-1}{4}$; $p=4n+3$, $b=\frac{p+1}{4}$.

Proof .(i) if $a\equiv b \pmod p$, it is obvious that equation (Ⅶ) is the solution of equation (Ⅵ) and (Ⅷ).

(ii) if $a\not\equiv b \pmod p$,

$x\equiv\pm(\frac{p-1}{2}-1) \pmod p$ is the solution of $x^2\equiv b+(\frac{p-1}{2}-1)^2-\frac{(p-1)^2}{4}\equiv b+1\times 2 \pmod p$;

$x\equiv\pm(\frac{p-1}{2}-2) \pmod p$ is the solution of $x^2\equiv b+(\frac{p-1}{2}-2)^2-\frac{(p-1)^2}{4}\equiv b+2\times 3 \pmod p$;

$x\equiv\pm(\frac{p-1}{2}-m) \pmod p$ is the solution of $x^2\equiv b+(\frac{p-1}{2}-m)^2-\frac{(p-1)^2}{4}\equiv b+m(m+1) \pmod p$, $m=1,2,\text{---},n-1$.

Therefore, $x\equiv\pm(\frac{p-1}{2}-m) \pmod p$ is the solution of equation (Ⅷ). □

$m(m+1)$ is the product of two consecutive integers, product of two consecutive integers single-digit just could be 0,2,6. In general, we need only check three numbers.

Example5. Solve these equation

(1) $x^2\equiv 11 \pmod{43}$; (2) $x^2\equiv 73 \pmod{127}$.

Solution: (1) $\frac{p-1}{2}=21$, $b=\frac{p+1}{4}=11$. $x^2\equiv 11 \pmod{43}$ is the benchmark equation for eqution $x\equiv\pm 21 \pmod{43}$. The solution of (1) is $x\equiv\pm 21 \pmod{43}$.

(2) $\frac{p-1}{2}=63$, $b=\frac{p+1}{4}=32$. $x^2\equiv 32 \pmod{127}$ is the benchmark equation for eqution $x\equiv\pm 63 \pmod{127}$, set $m(m+1)=127k+(73-32)=127k+41$. $k_{unit}=3, 5, 7$, such taht $k=7$, $127k+41=30\times 31$, $m=30$, $\frac{p-1}{2}-30=33$, The solution of (2) is $x\equiv\pm 33 \pmod{127}$.

4.2. The solution of quadratic congruence equation for module p^k

P is a prime number ,$x^2\equiv a \pmod{p^k}$,$(p, a)=1$. (Ⅸ)

Make (Ⅸ) as below system：

$$\begin{cases} f(x)=x^2-a\equiv 0 \pmod{p}, & ① \\ f(x)\equiv 0 \pmod{p^2}, & ② \\ \quad\cdots \quad\quad\cdots & \\ f(x)\equiv 0 \pmod{p^k}. & ⓚ \end{cases}$$

Lemma 2. Necessary and sufficient condition for equation (Ⅸ) has solution:
$f'(x_i)\,p^i t_i+f(x_i)\equiv 0 \pmod{p^{i+1}}$, $i=1, 2, \cdots, k-1$.

Since $f'(x)=2x$, $x_1\,p^i t_i+f(x_i)\equiv 0 \pmod{p^{i+1}}$. $2x_i t_i+\frac{f(x_i)}{p^i}\equiv 0 \pmod{p}$. （★）

$(x_i, p)=1$, $(2, p)=1$, $(2x_i, p)=1$, $i=1, 2, \cdots, k-1$. If equation (★) has only two solutions, it means anyone of equations ①, ②, …, ⓚ has only two solution, then the way to get the solution of quadratic congruence equation for module p^k is the same as module p (p is a prime number).

Theorem 11. p is a priem number, $(p^k, a)=1$, $x^2\equiv a \pmod{p^k}$ (Ⅸ)

(i) $a\equiv b \pmod{p^k}$, the solution of (Ⅸ) is $x\equiv\pm\frac{p^k-1}{2} \pmod{p^k}$;

(ii) $a\not\equiv b \pmod{p^k}$, the necessary and sufficient condition for euqtion (Ⅸ) has solution is $m(m+1)\equiv a-b \pmod{p^k}$. $m=1,2, \cdots, n-1$.

If that , the solution for equation (Ⅸ) is $x=\pm(\frac{p^k-1}{2}-m) \pmod{p^k}$, when $p^k=4n+1$, $b=-\frac{p-1}{4}$; $p^k=4n+3$, $b=\frac{p+1}{4}$.

Definition2. p is a prime number, for $\boldsymbol{x\equiv\pm\frac{p^k-1}{2}\ (\mathbf{mod}\ p^k)}$,$x^2\equiv b \pmod{p^k}$ is called its *benchmark equation*.

Example 6. Solving equation $x^2\equiv 11 \pmod{5^3}$.

Dissolve: $\frac{5^3-1}{2}=62$, $b=-\frac{5^3-1}{4}=-31$. For $x\equiv\pm 62 \pmod{5^3}$,$x^2\equiv -31 \pmod{5^3}$ is named as its benchmark equation.

$m(m+1)=5^3k+(a-b)=5^3k+6\times 7$. $k=0$, $m=6$, $\frac{5^3-1}{2}-m=62-6=56$.

The solution of the original equation is $x\equiv\pm 56 \pmod{5^3}$.

4.3. Mold is the solution of quadratic congruence equation of 2^k

$x^2\equiv a \pmod{2^k}$, $(2, a)=1$ (Ⅹ).

$k=1$, (Ⅹ) has the unique solution $x\equiv 1 \pmod 2$; $k=2$, the sufficient and necessary condition that (Ⅹ) is of solvability is: $a\equiv 1 \pmod{2^2}$. If this, the solution of (Ⅹ) is $x\equiv\pm 1 \pmod{2^2}$; $k\geq 3$, the sufficient and necessary condition that (Ⅹ) is of solvability is: $a\equiv 1 \pmod{2^3}$. If this, (Ⅹ) has 4 Solutions. If $x=\alpha$ is one solution of (Ⅹ), then all solutions of (Ⅹ) are $x\equiv\pm\alpha$, $\pm(\alpha+2^{k-1}) \pmod{2^k}$.

Definition3. for $x\equiv\pm(2k-1) \pmod{2^k}$,$x^2\equiv(2k-1)^2\equiv b \pmod{2^k}$ ($k\geq 3$) is called as its *benchmark equation*.

Theorem 12. $x^2\equiv a \pmod{2^k}$，$(2, a)=1$ (Ⅹ).

(i) if $a\equiv b\equiv(2k-1)^2 \pmod{2^k}$,the solutions of equation are $x\equiv\pm(2k-1)$and $x\equiv\pm(2k-1+2^{k-1}) \pmod{2^k}$.

(ⅱ) if $a\not\equiv b \pmod{2^k}$and the necessary and sufficient condition of equation having the solution is $(m+k)(m+k-1)\equiv k(k-1)+\frac{a-b}{4} \pmod{2^{k-2}}$,$x\equiv\pm[(2k-1)+2m]$and $\pm[(2k-1)+2m+2^{k-1}] \pmod{2^{k-2}}$ are called as the solutions of equation.

Proof. For $x^2\equiv(2k-1)^2\equiv 4k(k-1)+1\equiv b \pmod{2^k}$ ($k\geq 3$),$x\equiv\pm(2k-1) \pmod{2^k}$ are called as its solutions of equation.

(i) if $a\equiv b \pmod{2^k}$，the solutions of equation are $x\equiv\pm(2k-1)$ and $x\equiv\pm(2k-1+2^{k-1}) \pmod{2^k}$.

(ii) if $a\not\equiv b \pmod{2^k}$ and the solution of equation is $x\equiv\pm(2k-1)+2m \pmod{2^k}$, we can get

$[(2k-1)+2m]^2\equiv 4(m+k)(m+k-1)+1\equiv a \pmod{2^k}$.

When $b-a\equiv 4k(k-1)-4(m+k)(m+k-1) \pmod{2^k}$,$k\geq 3and8|(b-a)$, we have

$(m+k)(m+k-1)\equiv k(k-1)+\frac{a-b}{4} \pmod{2^{k-2}}$. □

$(m+k)(m+k-1)$ is called as the product of two consecutive integers; in general, only three numbers are checked out among ten numbers.

Example 7 Solve the following equation.

（1）$x^2\equiv 57 \pmod{2^6}$；(2) $x^2\equiv 145 \pmod{2^8}$.

Solution: (1) $k=6$, $2k-1=11$, $x^2\equiv 11^2\equiv 57 \pmod{2^6}$ is benchmark equation of $x\equiv\pm 11 \pmod{64}$.

The solution of (1) is $x\equiv\pm 11, \pm(11+2^5)\equiv\pm 11, \pm 21 \pmod{2^6}$.

(2) $k=8$, $2k-1=15$. $x^2\equiv 15^2\equiv 225 \pmod{2^8}$ is benchmark equation of $x\equiv\pm 15 \pmod{2^8}$.

$(m+k-1)(m+k)=(m+7)(m+8)=2^{k-2}n+k(k-1)+\frac{a-b}{4}=64n+36$，$n_{unit}=0, 4, 6$.

$n=6$，$64n+36=20\times 21$, $m+7=20$, $m=13$. $(2k-1)+2m=15+26=41$.

The solution of (2) is $x\equiv\pm 41, \pm(41+2^7)\equiv\pm 41, \pm 87 \pmod{2^8}$.

4.4.The sum of the squares of the two Numbers

The prime number p is expressed as $p=x^2+y^2$($p=4n+1$)，according to the following steps.

(1) Solve equations $x^2\equiv -1 \pmod{p}$.

$(-1)^{\frac{p-1}{2}}=(-1)^{2n}=1$,the equation has the solution. According to theorem 10, $x\equiv\pm x_1 \pmod{p}$ is the solutions of equation.

（2）Seek the values of x, y by Euclid algorithm.

Calculate $r=[\sqrt{p}+1]$，when$r_{n-1}<r$，$r_n<r$，$r_{n-2}>r$，make $x=r_n$，y= r_{n-1}，then $x^2+y^2=p$.

Example 8. Write 233 for the sum of the squares of the other two Numbers.

Answer: The solution of $x^2\equiv -1 \pmod{233}$ is $x\equiv\pm 89 \pmod{233}$.

$r=[\sqrt{233}+1]=16$. Take $x=13$, $y=8$, then $233=13^2+8^2$.

2	89, 233	
1	34，55	1
1	13，21	1
	8	

V. ORIGINAL ROOT

5.1. The relation among original root and the simplified residue system .quadratic residue

Lemma 3 . (*L.Euler*c riterion)Suppose p is odd prime numbers，

The necessary and sufficient condition for x is quadratic residue of mod p is：

$x^{\frac{p-1}{2}}-1\equiv 0(\mathrm{mod}p)$;

The necessary and sufficient condition for x is not quadratic residue of mod p is: $x^{\frac{p-1}{2}}+1\equiv 0(\mathrm{mod}p)$.

Theorem 13. If $j_{(p)}$， $p_{(p)}$， $g_{(p)}$ are the sets of simplified residue system .quadratic residue and original root of odd prime numbers p, $f_{(p)}=\complement_{j(p)}(p_{(p)}\cup g_{(p)})$ (where $\complement_{j(p)}$ represent complementary set).as in figure 1.

(i) If $p-1=2^{\alpha}$， then $g_{(p)}=\complement_{j(p)}(p_{(p)})$, that is $f_{(p)}=\Phi$.

(ii) If $p-1=2^{\alpha}\prod_{i=1}^{k}q_i^{\beta_i}$ ， q_i is odd prime numbers, then $g_{(p)}=\complement_{j(p)}(p_{(p)}\cup f_{(p)})$.

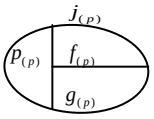


figure1

Proof. (i) $\varphi(\varphi(p))=\varphi(p-1)=\varphi(2^{\alpha})=2^{\alpha-1}$， $\mathrm{card}(g_{(p)})=2^{\alpha-1}$(card ($A$)represents the numbers of set A).

$x^{p-1}-1=x^{2^{\alpha}}-1=(x^{2^{(\alpha-1)}}-1)(x^{2^{(\alpha-1)}}+1)$.From Lemma 3，

$p_{(p)}=\{x|x^{2^{(\alpha-1)}}-1\equiv 0(\mathrm{mod}p)\}$， $\mathrm{card}(p_{(p)})=\frac{p-1}{2}=2^{\alpha-1}$， $\mathrm{card}(j_{(p)})=p-1=2^{\alpha}$.

$\mathrm{card}(j_{(p)})-\mathrm{card}(p_{(p)})=2^{\alpha}-2^{\alpha-1}=2^{\alpha-1}=\mathrm{card}(g_{(p)})$.

$g_{(p)}=\{x|x^{2^{(\alpha-1)}}+1\equiv 0(\mathrm{mod}p)\}=\complement_{j(p)}(p_{(p)})$.

(ii) $\varphi(p-1)=\varphi(2^{\alpha}\prod_{i=1}^{k}q_i^{\beta_i})=2^{(\alpha-1)}\prod_{i=1}^{k}q_i^{(\beta_i-1)}\prod_{i=1}^{k}(q_i-1)$ ，

$x^{2^{\alpha}\prod_{i=1}^{k}q_i^{\beta_i}}-1=(x^{2^{(\alpha-1)}\prod_{i=1}^{k}q_i^{\beta_i}}-1)(x^{2^{(\alpha-1)}\prod_{i=1}^{k}q_i^{\beta_i}}+1)$. mark $t_{(g_i)}=2^{(\alpha-1)}\prod_{i=1}^{k}q_i^{\beta_i}/q_i$,

$x^{2^{(\alpha-1)}\prod_{i=1}^{k}q_i^{\beta_i}}+1=(x^{t(q_1)}+1)(\sum_{i=0}^{q_1-1}(-1)^i x^{t(q_1)i})=(x^{t(q_2)}+1)(\sum_{i=0}^{q_2-1}(-1)^i x^{t(q_2)i})=\ldots=(x^{t(q_k)}+1)(\sum_{i=0}^{q_k-1}(-1)^i x^{t(q_k)i})$.

Original roots are not in $x^{t(q_i)}+1\equiv 0(\mathrm{mod}p)$， but in (Ⅺ).

$g_{(x)}=\{x|\sum_{i=0}^{q_i-1}(-1)^i x^{t(q_i)i}\equiv 0(\mathrm{mod}p), i=1,2,\ldots,k\}=\complement_{j(p)}(p_{(p)}\cup f_{(p)})$. (Ⅺ) □

Since $q_1,q_2,\ldots,q_k$ are co-prime， The number of equations in (Ⅺ) is not equal. From theorem 5， Seprate the factors not containing (ii) using (Ⅺ)， we have $g_{(x)}\equiv 0(\mathrm{mod}\ p)$.

Example 9. Solve the original roots of the following numbers.

（1）17； （2）211.

Answer: （1）$\varphi(\varphi(17))=\varphi(16)=8$. $x^{16}-1=(x^8-1)(x^8+1)\equiv 0(\mathrm{mod}17)$.

$j_{(17)}=\{\pm1,\pm2,\ldots,\pm8\}$, $p_{(17)}=\{\pm1,\pm2,\pm4,\pm8\}$, $g_{(17)}=\{\pm3,\pm5,\pm6,\pm8\}$.

（2）$\varphi(210)=\varphi(2)\varphi(3)\varphi(5)\varphi(7)=48$. $x^{210}-1=(x^{105}-1)(x^{105}+1)$.

$x^{105}+1=(x^{35}+1)(①)=(x^{21}+1)(②)=(x^{15}+1)(③)$.

①$=x^{70}-x^{35}+1$; ②$=x^{84}-x^{63}+x^{42}-x^{21}+1$; ③$=x^{90}-x^{75}+x^{60}-x^{45}+x^{30}-x^{15}+1$.

①∩②$=x^{56}+x^{49}-x^{35}-x^{28}-x^{21}+x^7+1$. ④

$g_{(x)}=$③∩④$=x^{48}-x^{47}+x^{46}-x^{42}+2x^{41}-x^{40}+x^{39}+x^{36}-x^{35}+x^{34}-x^{33}+x^{32}-x^{31}-x^{28}-x^{26}-x^{24}$
$-x^{22}-x^{20}-x^{17}+x^{16}-x^{15}+x^{14}-x^{13}+x^{12}+x^9-x^8+2x^7-x^6+x^5+x^2-x+1$ ⑤.

The 48 original roots of 211 are in $g_{(x)}\equiv 0(\mathrm{mod}211)$.

$x^{70}-x^{35}+1=(x^{14}-x^7+1)(x^8+x^7-x^5-x^4-x^3+x+1)$ (⑤), $j_{(211)}=\{\pm1,\pm2,\ldots,\pm105\}$.

$f_{(211)}=\{x|(x^{35}+1)(x^{14}-x^7+1)(x^8+x^7-x^5-x^4-x^3+x+1)\equiv 0(\mathrm{mod}211)\}$.

$p_{(211)}=\{1,-2,-3,4,5,6,-7,-8,9,-10,11,-12,13,14,-15,16,-17,-18,19,20,21,-22,$
$-23,24,25,-26,-27,-28,-29,30,-31,-32,-33,34,-35,36,37,-38,-39,-40,-41,$

－42,43,44,45,46,47,－48,49,－50,51,52,53,5455,56,－57,58,59,－60,－61,62,－63,64,65,66,
－67,－68,69,70,71,－72,73,－74,－75,76,－77,78,79,80,81,82，83,84,－85,－86,87,－88,－89, －90,
－91,－92,93,－94,95,96,－97,－98,99,100,101,－102,103,－104,105}.

{ $x|x^{35}+1\equiv 0(\mathrm{mod}211)$}={－1,－5,8,－11,12,－13,18,23,－25,27,28,40,42,－55,－58,60,63,－64,－65，
67,68,－71,－76,－79,82,86,－87,88,89,90,－96,97,98,102,104}.

{ $x|x^{14}-x^{7}+1\equiv 0(\mathrm{mod}211)$}= {－14,15,26,31,32,33,－34,38,－43,50,－54,－73,94,－101}.

{ $x|x^{8}+x^{7}-x^{5}-x^{4}-x^{3}+x+1\equiv 0(\mathrm{mod}211)$}={10,－19,－21,61,74,77,－83,－100}.

$g_{(211)}$= {2,3,－4,－6,7,－9,－16,17,－20,22,－24,29,－30,35,－36,－37,39,41,－44,－45, －46,－47,48,
－49,－51－52,－53,－56,57,－59,－62,－66,－69,－70, 72,75,－78,－80,－81,－84,85,91,92,－93,－
95,－99,－103,－105}.

5.2. The application of original root in factoring

If $f(2t,d_t)=\sum_{i=0}^{2t/d_t}(-1)^i x^{2t-id_t}$,(Ⅻ) where d_t is the approximate number of t，$(4t+2d_t+1)$ Is a prime number.

The index number of x *is* arithmetic progression with tolerance d_t and coefficient $(-1)^i$ If number of terms of (Ⅻ) is composite number，then (Ⅻ) is dissoluble. We discuss the case when the number of items of (Ⅻ) is odd prime numbers.

d_t is the approximate number of t，The index number of x *is* arithmetic progression with tolerance d_t，d_t are different，the tolerance of the sequence are different，the number of terms of (Ⅻ) are different ,Denote $T_{(t)}$ is the number of approximate number of t, the expression number of (Ⅻ) is $T_{(t)}$.

Theorem14. if $P(P=4t+2d_t+1)$ is a prime number，

(i) If $\varphi(4t+2d_t)=2t$，then (Ⅻ) is not decomposable;

(ii) If $\varphi(4t+2d_t)<2t$, then (Ⅻ) is decomposable.

Proof. (i) $f(2t,d_t)=\sum_{i=0}^{2t/d_t}(-1)^i x^{2t-id_t}=\dfrac{x^{2t+d_t}+1}{x^{d_t}+1}=\dfrac{x^{4t+2d_t}-1}{(x^{d_t}+1)(x^{2t+d_t}-1)}$.

The original root of P is not in $x^{2t+d_t}-1\equiv 0(\mathrm{mod}\ p)$ and $x^{d_t}+1\equiv 0(\mathrm{mod}\ p)$. if (Ⅻ)can factor，then the number of the original root of (Ⅻ) is smaller than $2t$. this is contradict with $\varphi(4t+2d_t)=2t$. (i) is held.

(ii) $g(x)$ is polynomial with integer coefficients. $\varphi(4t+2d_t)<2t$，there exists polynomial with integer coefficients $f(x)$ in (Ⅻ)，such that $f(2t,d_t)=f(x)g(x)$ hold. Therefore (Ⅻ) is decomposable. (ii) hold. □

Example10. distinguish if this following formulas are decomposable，decompose those can be decomposable.

(1) $x^{12}-x^{10}+x^{8}-x^{6}+x^{4}-x^{2}+1$;　　(2) $x^{804}-x^{603}+x^{402}-x^{201}+1$.

Answer: (1) 2(12+2)+1=29, $\varphi(28)=12$, (1)is not decomposable.

(2) 2(804+201)+1=2011, $\varphi(2010)=528<804$，(2) is decomposable..

$x^{2010}-1=(x^{1005}-1)(x^{1005}+1)$,

$x^{1005}+1=(x^{201}+1)(x^{804}-x^{603}+x^{402}-x^{201}+1)=(x^{335}+1)(x^{670}-x^{335}+1)$.

$x^{804}-x^{603}+x^{402}-x^{201}+1$and $x^{670}-x^{335}+1$factor is $x^{536}+x^{469}-x^{335}-x^{268}-x^{201}+x^{67}+1$.

$x^{804}-x^{603}+x^{402}-x^{201}+1=(x^{536}+x^{469}-x^{335}-x^{268}-x^{201}+x^{67}+1)(x^{268}-x^{201}+x^{134}-x^{67}+1)$.

REFERENCES

[1]. Hua, Loo-Keng. (1979). *An introduction to number theory* (In Chinese).Beijing: Science Press.

[2]. Min Sihe Yan Shijian. (2003) *Elementary number theory*(In Chinese). Beijing: Higher Education Press.

[3]. Xiong, Q. (1982). *Elementary number theory* (In Chinese). Wuhan: Hubei Education Press.

[4]. Song, K. (2007). *Elementary number theory* (In Chinese). Beijing: China Drama Press.

初等数论的几个基础问题

宋开福

中国湖北宜昌东湖高中 邮编 443100 邮箱 skf08@sina.com

摘　要：给出不定方程 $x^2+y^2=z^2$ 的一条性质；给出一元同余方程、二次同余方程的解；揭示奇素数 p 的原根与简化剩余系、平方剩余的关系.

关键词：勾股数；一元同余方程；二次同余方程；原根.

MR(2000)：08B10；**1CLC:** 0156.1.

1．勾股数

定理 1　x、y、$z\in Z_+$(Z 为整数集)，$x>2$，方程 $x^2+y^2=z^2$ (Ⅰ), 至少有一组解.

证 $x^2=z^2-y^2=(z+y)(z-y)$.

(i) $x=2m+1$，$m\in Z_+$时，$\forall$ m 使$(z+y)(z-y)=(2m+1)^2$ 成立.

令 $z-y=1$，$z+y=(2m+1)^2$,得到 $x=2m+1$，$y=2m^2+2m$, $z=2m^2+2m+1$.

(ii) $x=2m$，且 $m\geq 2$ 时，$\forall$ m 使$(z+y)(z-y)=4m^2$ 成立.

令 $z-y=2$，$z+y=2m^2$，得到 $x=2m$，$y=m^2-1$，$z=m^2+1$. □

满足(Ⅰ)的三个正整数 x、y 和 z 叫做**勾股数**.

例 1 由下列各数写出勾股数.

（1）37，　（2）40.

解 （1）令 $x=2m+1=37$，得 $m=18$．$y=2m^2+2m=684$，$z=y+1=685$. 那么 $37^2+684^2=685^2$；

令 $z=2m^2+2m+1=37$，那么 $m\notin Z$；令 $y=m^2-1=37$，那么 $m\notin Z$；

令 $z=m^2+1=37$，得 $m=6$．$x=12$，$y=35$. 那么 $12^2+35^2=37^2$.

所以由 37 可写出两组勾股数.

（2）令 $x^2=(2m)^2=4m^2=1\times1600=2\times800=4\times400=5\times320=8\times200=10\times160=16\times100$

$=20\times80=25\times64=32\times50=40\times40$.

令 $z-y=2$，$z+y=2m^2=800$, 那么 $x=40$，$y=399$，$z=401$；

令 $z-y=4$，$z+y=2m^2=400$, 那么 $x=40$，$y=198$，$z=202$；

令 $z-y=8$，$z+y=2m^2=200$, 那么 $x=40$，$y=96$，$z=104$；

令 $z-y=10$，$z+y=2m^2=160$, 那么 $x=40$，$y=75$，$z=85$；

令 $z-y=16$，$z+y=2m^2=100$, 那么 $x=40$，$y=42$，$z=58$；

令 $z-y=20$，$z+y=2m^2=80$, 那么 $x=40$，$y=30$，$z=50$；

令 $z-y=32$，$z+y=2m^2=50$, 那么 $x=40$，$y=9$，$z=41$；

令 $z=m^2+1=5$，$m=2$，那么 $4^2+3^2=5^2$，$32^2+24^2=40^2$. $x=32$，$y=24$，$z=40$.

所以由 40 可写出 8 组勾股数.

定理 2　x、y、z、$l\in Z_+$，方程 $x^2+y^2+z^2=l^2$ 至少有一组解.

证 $1^2+2^2+2^2=3^2$. $x>2$, 由定理 1，

$x^2+y^2=z_1^2$，$z_1>2$；$z_1^2+z^2=l^2$.所以 $x^2+y^2+z^2=l^2$. □

$x\geq 3$,

$$\begin{cases} x=2m+1 \\ y=2m^2+2m \\ z=\dfrac{1}{2}[(2m^2+2m+1)^2-1] \\ l=\dfrac{1}{2}[(2m^2+2m+1)^2+1]; \end{cases} \quad \begin{cases} x=2m(m\text{ 是偶数}) \\ y=m^2-1 \\ z=\dfrac{1}{2}[(m^2+1)^2-1] \\ l=\dfrac{1}{2}[(m^2+1)^2+1]; \end{cases} \quad \begin{cases} x=2m(m\text{ 是奇数}) \\ y=m^2-1 \\ z=\dfrac{1}{4}(m^2+1)^2-1 \\ l=\dfrac{1}{4}(m^2+1)^2+1. \end{cases}$$

定理 3 $x_i\in Z_+$，$n\geq 3$，方程 $x_1^2+x_2^2+\cdots+x_n^2=x_{n+1}^2$ 至少有一组解.

2．同余理论

用同余理论给定理 4 证明.

定理 4 若 $a,b\in Z$，且不全为 0，则存在 x，$y\in Z$ 使 $ax+by=(a，b)$成立.

证 由 $ax+by=(a，b)$,得 $\frac{a}{(a,b)}x+\frac{b}{(a,b)}y=1$，记 $m=\frac{a}{(a,b)}$，$n=\frac{b}{(a,b)}$，有 $mx+ny=1$.

设 A 是 m 的完全剩余系，因为$(m，n)=1$, nA 也是关于模 m 的完全剩余系. 那么 nA 中存在 na_i 与 A 中的 1 使 $na_i\equiv 1(\mathrm{mod}m)$成立.取 $y=a_i$，那么 $x=\frac{1-ny}{m}\in Z$. □

3．一元同余方程

3.1．素数模的高次同余方程

引理 1 (*J.L.Lagrange* 定理)$n(<p)$次同余方程 $f(x)\equiv 0(\mathrm{mod}p)$ $((p，a_n)=1)$ (Ⅱ),

有 n 个不相同解的充要条件是：$x^p-x\equiv q(x)f(x)\ (\mathrm{mod}\ p)$.

定理 5 $n(<p)$次同余方程 $f(x)\equiv 0(\mathrm{mod}p)$ (Ⅱ),有解的充要条件是：

$f(x)=q(x)r(x)\equiv 0\ (\mathrm{mod}\ p)$，且 $x^p-x=g(x)f(x)+r(x)\equiv 0(\mathrm{mod}p)$.

如果 $r(x)$的次数为 m，那么(Ⅱ)有 m 个不相同的解. $m\leq n$.

证 $f(x)=q(x)r(x)\equiv 0\ (\mathrm{mod}\ p)$，$x^p-x=g(x)f(x)+r(x)\equiv r(x)[\ g(x)q(x)+1]\equiv 0\ (\mathrm{mod}p)$. 由引理 1, $r(x)\equiv 0\ (\mathrm{mod}p)$有 m 个不相同的解.即(Ⅱ)有 m 个不相同的解.必要性显然. □

例 2 解方程 $f(x)\equiv 0\ (\mathrm{mod}\ 7)$.

$f(x)=2x^{17}+6x^{16}+x^{14}+5x^{12}+3x^{11}+2x^{10}+x^9+5x^8+2x^7+3x^5+4x^4+6x^3+4x^2+x+4$.

解 $f(0)\neq 0(\mathrm{mod}\ 7)$，$f(x)\equiv(x^6-1)\,g_1(x)+r_1(x)\ (\mathrm{mod}\ 7)$. 这里,

$g_1(x)=2x^{11}-x^{10}+x^8-2x^6-2x^5+x^4+x^3-x^2+2x-2$, $r_1(x)=x^5-2x^4+3x^2+3x+2$.

$x^6-1\equiv r_1(x)\,g_2(x)+r_2(x)\ (\mathrm{mod}\ 7)$.这里, $g_2(x)=x+2$, $r_2(x)\equiv x^4+x^3+3x^2-2x-3(\mathrm{mod}\ 7)$.

$r_1(x)\equiv r_2(x)\,g_3(x)\ (\mathrm{mod}\ 7)$, 即 $r_3(x)\equiv 0\ (\mathrm{mod}\ 7)$.

$r_2(x)\equiv 0\ (\mathrm{mod}\ 7)$的解是 $f(x)\equiv 0\ (\mathrm{mod}\ 7)$不相同的解.

$x^6-1\equiv(x^2-x-2)r_2(x)\ (\mathrm{mod}\ 7)$中，$x^3-x^2-2x\equiv 0\ (\mathrm{mod}\ 7)$的解是 $x\equiv 0,\ -1,\ 2(\mathrm{mod}\ 7)$.

$f(x)\equiv 0\ (\mathrm{mod}\ 7)$不相同的解与 $x^3-x^2-2x\equiv 0\ (\mathrm{mod}\ 7)$的解互补.

$f(x)\equiv 0\ (\mathrm{mod}\ 7)$不相同的解是 $x\equiv 1,-2,\pm 3\ (\mathrm{mod}\ 7)$.

3.2．方程组 $\begin{cases}x\equiv a(\mathrm{mod}m)\\ x\equiv b(\mathrm{mod}n)\end{cases}$ (Ⅲ)，**有解的充要条件**

定理 6 方程组 $\begin{cases}x\equiv a(\mathrm{mod}m)\\ x\equiv b(\mathrm{mod}n)\end{cases}$ (Ⅲ)，有解的充要条件是:

$a+mt\equiv b\ (\mathrm{mod}\ n)$ (或 $b+nt\equiv a\ (\mathrm{mod}\ m)$)，$t\in \boldsymbol{Z}$.

若此，(Ⅲ)的解是 $x\equiv a+mt(\mathrm{mod}[m,\ n])$ (或 $x\equiv b+nt(\mathrm{mod}[m,\ n])$).

证 $x\equiv b\equiv a+mt(\mathrm{mod}\ n)$，$x\equiv a+mt(\mathrm{mod}\ m)$. 那么 $x\equiv a+mt(\mathrm{mod}[m,\ n])$.

$x\equiv a+mt(\mathrm{mod}[m,\ n])$，得 $x\equiv a+mt(\mathrm{mod}\ n)$， 又 $x\equiv b(\mathrm{mod}\ n)$. 则 $a+mt\equiv b\ (\mathrm{mod}\ n)$. □

定理 7，方程组 $\begin{cases}x\equiv b_1\ (\mathrm{mod}m_1)\\ \cdots\\ x\equiv b_n\ (\mathrm{mod}m_n)\end{cases}$ (Ⅳ), 有解的充要条件是：

$b_1+m_1t_1+[m_1,m_2]\,t_2+\ldots+[\,m_1，\ m_2，\ \ldots，\ m_i]\,t_i\equiv b_{i+1}(\mathrm{mod}m_{i+1})$，$i=1,2，\ \ldots,n-1$.

若此，(Ⅳ)的解是：$x\equiv b_1+m_1t_1+[m_1,m_2]\,t_2+\ldots+[\,m_1，\ m_2，\ \ldots，\ m_{n-1}]\,t_{n-1}(\mathrm{mod}[m_1，\ m_2，\ \ldots，\ m_n])$.

证 由定理 6，$n=1,2$ 时命题成立. 假定 $n=k$ 时命题成立.

(Ⅳ)解是：$x\equiv b_1+m_1t_1+[m_1,m_2]\ t_2+\ldots+[\ m_1,\ m_2,\ldots,m_{k-1}]\ t_{k-1}(\mathrm{mod}[m_1,\ m_2,\ldots,m_k])$.

t_{k-1} 满足方程 $b_1+m_1t_1+[m_1,m_2]\ t_2+\ldots+[\ m_1,\ m_2,\ \ldots,\ m_{k-1}]\ t_{k-1}\equiv b_k(\mathrm{mod}m_k)$.$n=k+1$ 时，得

$$\begin{cases} x\equiv b_{k+1}(\mathrm{mod}m_{k+1}) \\ x\equiv b_1+m_1t_1+[m_1,m_2]\ t_2+\ldots+[\ m_1,\ m_2,\ \ldots,\ m_{k-1}]\ t_{k-1}(\mathrm{mod}[m_1,\ m_2,\ \ldots,\ m_k]). \end{cases} \quad (\dagger)$$

由定理 6，t_k 满足方程 $b_1+m_1t_1+[m_1,m_2]\ t_2+\ldots+[\ m_1,\ m_2,\ \ldots,\ m_i]\ t_i\equiv b_{i+1}(\mathrm{mod}m_{i+1})$. (†)的解就是(Ⅳ)的解，从而(Ⅳ)的解是:

$x\equiv b_1+m_1t_1+[m_1,m_2]\ t_2+\ldots+[\ m_1,\ m_2,\ \ldots,\ m_k]\ t_k(\mathrm{mod}[m_1,\ m_2,\ \ldots,\ m_{k+1}])$.

即 $n=k+1$，命题成立. □

例 3 解方程组 $\begin{cases} x\equiv 1(\mathrm{mod}15) \\ x\equiv -2(\mathrm{mod}12) \\ x\equiv 6(\mathrm{mod}10) \end{cases}$.

解 $1+15\ t_1\equiv -2(\mathrm{mod}\ 12)$， $t_1=-1$；$1+15\ t_1+60\ t_2\equiv 6(\mathrm{mod}\ 10)$，$t_2=0$.

方程组的解是 $x\equiv 1-15\equiv -14\equiv 46\ (\mathrm{mod}\ 60)$.

3.3．同余方程组模的扩张

$f(x)=\sum_{i=0}^{n} a_i x^{n-i}$, $a_i\in \boldsymbol{Z}$，$a_0\neq 0$，$(a_0, a_1,\ldots,a_n)=1$，$f(x)$为最简整系数多项式.

定理 8 方程组 $\begin{cases} f\equiv r_1\ (\mathrm{mod}m) \\ f\equiv r_2(\mathrm{mod}1n) \end{cases}$ (Ⅴ)，有解的充要条件是:$mt+\ r_1\equiv r_2\ (\mathrm{mod}\ n)$ (或 $nt+\ r_2\equiv r_1\ (\mathrm{mod}\ m)$).

若此，(Ⅴ)的解是:. $f\equiv mk+\ r_1\equiv r_2\ (\mathrm{mod}[\mathrm{m},\ n])$.

这里，f，r_1，r_2，t, m，n 都是最简整系数多项式，$\partial^\circ r_1<\partial^\circ m$，$\partial^\circ r_2<\partial^\circ n$($\partial^\circ f(x)$为 x 的次数).

证 $f\equiv r_2\equiv mt+\ r_1\ (\mathrm{mod}\ n)$, $x\equiv mt+\ r_1\ (\mathrm{mod}\ m)$. 则 $f\equiv mt+\ r_1\ (\mathrm{mod}[m,\ n])$.

$f\equiv mt+\ r_1\ (\mathrm{mod}[m,\ n])$，得 $f\equiv mt+\ r_1\ (\mathrm{mod}\ n)$，$f\equiv r_2\ (\mathrm{mod}\ n)$. 则 $mt+\ r_1\equiv r_2\ (\mathrm{mod}\ n)$. □

例 4 解方程组 $\begin{cases} f(x)\equiv r_1(\mathrm{mod}\ g_1(x)) & ① \\ f(x)\equiv r_2(\mathrm{mod}\ g_2(x)) & ② \\ f(x)\equiv r_3(\mathrm{mod}\ g_3(x)) & ③ \end{cases}$. 这里

$r_1(x)=13x^2-8x+26$, $g_1(x)=x^3+2x^2+3$; $r_2(x)=105x-60$, $g_2(x)=x^2-4x+2$; $r_3(x)=52$, $g_3(x)=x+2$.

解 设 $g_1(x)\ p(x)+\ r_1(x)\equiv r_2(\mathrm{mod}\ g_2(x))$. 即$(22x-9)\ p(x)-61x+60\equiv 0(\mathrm{mod}\ g_2(x))$.

$-61x+60\neq 0(\mathrm{mod}\ g_2(x))$，$\partial^\circ(22x-9)=1$，$\partial^\circ(g_2(x))=2$. 设 $p(x)=ax+b$.

$(22x-9)(\ ax+b)-61x+60\equiv 22ax^2-(9a-22b+61)x-(9b-60)\equiv c(x^2-4x+2)(\mathrm{mod}\ g_2(x))$.

由 $22a=c$，$9a-22b+61=4c$，$9b-60=-2c$.得 a=3，b=−8.所以 $p(x)=3x-8$.

①，②的解是: $f(x)\equiv g_1(x)\ p(x)+\ r_1(x)\equiv 3\ x^4-2\ x^3-3\ x^2+\ x+2(\mathrm{mod}\ g_1(x)g_2(x))$.

又因为 $3\ x^4-2\ x^3-3\ x^2+\ x+2\equiv 52(\mathrm{mod}\ g_3(x))$.

所以原方程组的解为: $f(x)\equiv 3\ x^4-2\ x^3-3\ x^2+\ x+2(\mathrm{mod}\ g_1(x)g_2(x)g_3(x))$.

4．二次同余方程的解

4.1.奇素数模 p 的二次同余方程解

定理 9 $x^2\equiv b$（$\mathrm{mod}\ p$）(Ⅵ)， $x\equiv\pm\dfrac{p-1}{2}\ (\mathrm{mod}\ p)$ (Ⅶ)，(Ⅶ)是(Ⅵ)的解(p 为素数).

这里，$p=4n+1$，$b=-\dfrac{p-1}{4}$；$p=4n+3$，$b=\dfrac{p+1}{4}$.

证（i）$p=4n+1$，$x^2-b\equiv\dfrac{(p-1)^2}{4}+\dfrac{p-1}{4}\equiv\dfrac{p(p-1)}{4}\equiv 0\ (\mathrm{mod}\ p)$;

（ii）$p=4n+3$，$x^2-b\equiv\frac{(p-1)^2}{4}-\frac{p+1}{4}\equiv\frac{p(p-3)}{4}\equiv 0(\text{mod } p)$.

由引理 1，(Ⅶ)是(Ⅵ)的解. □

定义 1 p 为素数，$x^2\equiv b \pmod p$叫做 $\boldsymbol{x\equiv\pm\frac{p-1}{2}}$ **(mod *p*)的基准方程**.

定理 10 p 为素数，$(p, a)=1$, $x^2\equiv a \pmod p$. (Ⅷ)

(ⅰ) $a\equiv b \pmod p$，(Ⅷ)的解是 $x\equiv\pm\frac{p-1}{2} \pmod p$.

（ii）$a\not\equiv b \pmod p$，(Ⅷ)有解的充要条件是: $m(m+1)\equiv a-b \pmod p$. $m=1,2,\ldots,n-1$.

若此，(Ⅷ)的解是: $x\equiv\pm(\frac{p-1}{2}-m) \pmod p$.

这里，$p=4n+1$，$b=-\frac{p-1}{4}$；$p=4n+3$，$b=\frac{p+1}{4}$.

证（ⅰ）当 $a\equiv b \pmod p$，显然(Ⅶ)是(Ⅵ)的解也是(Ⅷ)的解.

（ii）当 $a\not\equiv b \pmod p$，

$x\equiv\pm(\frac{p-1}{2}-1) \pmod p$是 $x^2\equiv b+(\frac{p-1}{2}-1)^2-\frac{(p-1)^2}{4}\equiv b+1\times 2 \pmod p$的解;

$x\equiv\pm(\frac{p-1}{2}-2) \pmod p$是 $x^2\equiv b+(\frac{p-1}{2}-2)^2-\frac{(p-1)^2}{4}\equiv b+2\times 3 \pmod p$的解; …;

$x\equiv\pm(\frac{p-1}{2}-m) \pmod p$是 $x^2\equiv b+(\frac{p-1}{2}-m)^2-\frac{(p-1)^2}{4}\equiv b+m(m+1) \pmod p$的解, $m=1,2,\ldots,n-1$.

所以，$x\equiv\pm(\frac{p-1}{2}-m) \pmod p$是(Ⅷ)的解. □

$m(m+1)$是两个连续整数的乘积，两个连续整数积的个位数只是 0，2，6. 一般情况下，某 10 之间只需检验 3 个数.

例 5 解下列方程.

(1) $x^2\equiv 11 \pmod{43}$; (2) $x^2\equiv 73 \pmod{127}$.

解 (1) $\frac{p-1}{2}=21$, $b=\frac{p+1}{4}=11$. $x^2\equiv 11(mod\ 43)$是方程 $x\equiv\pm 21 \pmod{43}$的基准方程.

所以(1)的解是： $x\equiv\pm 21 \pmod{43}$.

(2) $\frac{p-1}{2}=63$，$b=\frac{p+1}{4}=32$. $x^2\equiv 32 \pmod{127}$是 $x\equiv\pm 63 \pmod{127}$的基准方程.

$m(m+1)=127k+(73-32)=127k+41$. $k_{个位}=3, 5, 7$.那么 $k=7$.

$127k+41=30\times 31$, $m=30$, $\frac{p-1}{2}-30=33$.

(2)的解是 $x\equiv\pm 33 \pmod{127}$.

4.2.模为 p^k 的二次同余方程的解

P 为素数，$x^2\equiv a(\text{mod } p^k)$,$(p, a)=1$. (Ⅸ)

(Ⅸ)写成如下方程组：

$$\begin{cases} f(x)=x^2-a\equiv 0 \pmod p, & ① \\ f(x)\equiv 0 \pmod{p^2}, & ② \\ \cdots \quad \cdots, & \\ f(x)\equiv 0 \pmod{p^k}. & ⓚ \end{cases}$$

引理 2 (Ⅸ)有解的充要条件是: $f'(x_i)\,p^i\,t_i+f(x_i)\equiv 0 \pmod{p^{i+1}}$, $i=1, 2, \ldots, k-1$.

由 $f'(x)=2x,\ x_1 p^i t_i+ f(x_i)\equiv 0 \pmod{p^{i+1}}$. $2x_i t_i + \dfrac{f(x_i)}{p^i}\equiv 0 \pmod p$. （★）

（x_i，p)=1, (2, p)=1, (2 x_i，p)=1, i=1, 2, …, k－1. 若(★)有解, 只有两解. 即①, ②, …, ⓚ有解且都只有两解. 这样，模为 p 与模为 p^k 的二次同余方程有相同的解题方法.

定理 11 p 为素数，(p^k, a)=1, $x^2\equiv a \pmod{p^k}$. （Ⅸ）

(i)若 $a\equiv b \pmod{p^k}$, (Ⅸ)的解是 $x=\pm\dfrac{p^k-1}{2} \pmod{p^k}$;

(ii)若 $a\not\equiv b \pmod{p^k}$，(Ⅸ)有解的充要条件是: $m(m+1)\equiv a-b \pmod{p^k}$. m =1,2，…, n -1.

若此，(Ⅸ)的解是 $x=\pm(\dfrac{p^k-1}{2}-m) \pmod{p^k}$.

这里，p^k =4n+1，$b=-\dfrac{p-1}{4}$；p^k =4n+3，$b=\dfrac{p+1}{4}$.

定义 2 p 为素数， $x^2\equiv b \pmod{p^k}$叫做 $\boldsymbol{x\equiv\pm\dfrac{p^k-1}{2}}$ **(mod $\boldsymbol{p^k}$)的基准方程**.

例 6 解方程 $x^2\equiv 11 \pmod{5^3}$.

解 $\dfrac{5^3-1}{2}$ =62 , $b=-\dfrac{5^3-1}{4}=-31$. $x^2\equiv -31 \pmod{5^3}$是方程 $x\equiv\pm 62 \pmod{5^3}$的基准方程.

$m(m+1)=5^3k+(a-b)=5^3k+6\times 7$. k=0, m=6, $\dfrac{5^3-1}{2}-m=62-6=56$.

原方程的解是 $x\equiv\pm 56 \pmod{5^3}$.

4.3.模为 2^k 的二次同余方程的解

$x^2\equiv a \pmod{2^k}$，(2, a)=1 (Ⅹ).

k=1, (Ⅹ)有唯一解 $x\equiv 1 \pmod 2$；k=2, (Ⅹ)有解的充要条件是: $a\equiv 1 \pmod{2^2}$. 若此，(Ⅹ)的解是 $x\equiv\pm 1 \pmod{2^2}$；$k\geq 3$，(Ⅹ)有解的充要条件是: $a\equiv 1 \pmod{2^3}$. 若此，(Ⅹ)有 4 个解. 若 $x=\alpha$ 是(Ⅹ)的一个解，(Ⅹ)的所有解是 $x\equiv\pm\alpha$，$\pm(\alpha+2^{k-1}) \pmod{2^k}$.

定义 3 $x^2\equiv(2k-1)^2\equiv b \pmod{2^k}$ ($k\geq 3$) 叫做 $\boldsymbol{x\equiv\pm(2k-1) \pmod{2^k}}$**的基准方程.**

定理 12 $x^2\equiv a \pmod{2^k}$，(2, a)=1 (Ⅹ).

(i)若 $a\equiv b\equiv(2k-1)^2 \pmod{2^k}$, 那么(Ⅹ)的解是: $x\equiv\pm(2k-1),\ \pm(2k-1+2^{k-1}) \pmod{2^k}$.

(ⅱ)若 $a\not\equiv b \pmod{2^k}$，那么(Ⅹ)有解的充要条件是：

$(m+k)(m+k-1)\equiv k(k-1)+\dfrac{a-b}{4} \pmod{2^{k-2}}$.

若此，(Ⅹ)的解是：$x\equiv\pm[(2k-1)+2m],\ \pm[(2k-1)+2m+2^{k-1}] \pmod{2^{k-2}}$.

证 $x\equiv\pm(2k-1) \pmod{2^k}$是 $x^2\equiv(2k-1)^2\equiv 4k(k-1)+1\equiv b \pmod{2^k}$ ($k\geq 3$)的解.

(i)若 $a\equiv b \pmod{2^k}$， $x\equiv\pm(2k-1)$，$\pm(2k-1+2^{k-1}) \pmod{2^k}$是(Ⅹ)的解.

(ii)若 $a\not\equiv b \pmod{2^k}$， $x\equiv\pm(2k-1)+2m \pmod{2^k}$是(Ⅹ)的解，则

$[(2k-1)+2m]^2\equiv 4(m+k)(m+k-1)+1\equiv a \pmod{2^k}$.

由 $b-a\equiv 4k(k-1)-4(m+k)(m+k-1) \pmod{2^k}$及 $k\geq 3$，$8|(b-a)$，得到

$(m+k)(m+k-1)\equiv k(k-1)+\dfrac{a-b}{4} \pmod{2^{k-2}}$. □

$(m+k)(m+k-1)$是两个连续整数的积，一般情况下，某 10 之间只需检验 3 个数.

例 7 解下列方程.

（1）$x^2\equiv 57 \pmod{2^6}$；(2) $x^2\equiv 145 \pmod{2^8}$.

解 (1) k=6, $2k-1$=11, $x^2\equiv 11^2\equiv 121\equiv 57 \pmod{2^6}$是 $x\equiv\pm 11 \pmod{64}$的基准方程.

(1)的解是 $x\equiv\pm 11,\ \pm(11+2^5)\equiv\pm 11,\ \pm 21 \pmod{2^6}$.

(2)　k=8, $2k$－1=15. $x^2\equiv 15^2\equiv 225 \pmod{2^8}$是 $x\equiv\pm 15 \pmod{2^8}$的基准方程.

$(m+k-1)(m+k)=(m+7)(m+8)=2^{k-2}n+k(k-1)+\dfrac{a-b}{4}=64n+36$，$n$ 个位=0, 4, 6.

n=6，$64n+36=20\times 21$, $m+7=20$, m=13. $(2k-1)+2m=15+26=41$.

(2)的解是 $x\equiv\pm 41, \pm(41+2^7)\equiv\pm 41, \pm 87 \pmod{2^8}$.

4.4.两个数的平方和

把素数 p 表示为 $p=x^2+y^2(p=4n+1)$，按如下步骤.

(1)　解方程 $x^2\equiv -1 \pmod p$.

$(-1)^{\frac{p-1}{2}}=(-1)^{2n}=1$, $x^2\equiv -1 \pmod p$有解.由定理 10，求其解 $x\equiv\pm x_1 \pmod p$.

（2）用 *Euclid* 算法求 x, y 的值.

计算 $r=[\sqrt{p}+1]$，当 $r_{n-1}<r$，$r_n<r$，$r_{n-2}>r$ 时，

取 $x=r_n$，$y=r_{n-1}$，则 $x^2+y^2=p$.

例 8　将 233 表作两个数的平方和.

解　$x^2\equiv -1 \pmod{233}$的解是 $x\equiv\pm 89 \pmod{233}$. $r=[\sqrt{233}+1]=16$.

取 x=13, y=8, 则 $233=13^2+8^2$.

2	89, 233	
1	34，55	1
1	13，21	1
	8	

5．原根

5.1.原根与简化剩余系、平方剩余的关系

引理 3 (*L.Euler* 判别条件)设 p 为奇素数，

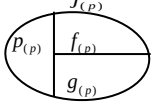
x 是模 p 的平方剩余的充要条件是：$x^{\frac{p-1}{2}}-1\equiv 0 \pmod p$;

x 是模 p 的平方非剩余的充要条件是：$x^{\frac{p-1}{2}}+1\equiv 0 \pmod p$.

定理 13 设 $j_{(p)}$, $p_{(p)}$, $g_{(p)}$分别是奇素数 p 的简化剩余系、平方剩余系、原根所组成的集合，$f_{(p)}=\complement_{j(p)}(p_{(p)}\cup g_{(p)})$ (这里$\complement_{j(p)}$表示补集).如图 1

(i)如果 $p-1=2^{\alpha}$，那么 $g_{(p)}=\complement_{j(p)}(p_{(p)})$，即 $f_{(p)}=\Phi$.

(ii)如果 $p-1=2^{\alpha}\prod_{i=1}^{k}q_i^{\beta_i}$，$q_i$ 为奇素数，那么 $g_{(p)}=\complement_{j(p)}(p_{(p)}\cup f_{(p)})$.



如图 1

证　(i) $\varphi(\varphi(p))=\varphi(p-1)=\varphi(2^{\alpha})=2^{\alpha-1}$，$\mathrm{card}(g_{(p)})=2^{\alpha-1}$. (card (*A*)表示集合 *A* 元素的个数)

$x^{p-1}-1=x^{2^{\alpha}}-1=(x^{2^{(\alpha-1)}}-1)(x^{2^{(\alpha-1)}}+1)$.由引理 3，

$p_{(p)}=\{x\mid x^{2^{(\alpha-1)}}-1\equiv 0 \pmod p\}$，$\mathrm{card}(p_{(p)})=\dfrac{p-1}{2}=2^{\alpha-1}$，$\mathrm{card}(j_{(p)})=p-1=2^{\alpha}$.

$\mathrm{card}(j_{(p)})-\mathrm{card}(p_{(p)})=2^{\alpha}-2^{\alpha-1}=2^{\alpha-1}=\mathrm{card}(g_{(p)})$.

$g_{(p)}=\{x\mid x^{2^{(\alpha-1)}}+1\equiv 0 \pmod p\}=\complement_{j(p)}(p_{(p)})$.

(ii)　$\varphi(p-1)=\varphi(2^{\alpha}\prod_{i=1}^{k}q_i^{\beta_i})=2^{(\alpha-1)}\prod_{i=1}^{k}q_i^{(\beta_i-1)}\prod_{i=1}^{k}(q_i-1)$ ，，

$x^{2^{\alpha}\prod_{i=1}^{k}q_i^{\beta_i}}-1=(x^{2^{(\alpha-1)}\prod_{i=1}^{k}q_i^{\beta_i}}-1)(x^{2^{(\alpha-1)}\prod_{i=1}^{k}q_i^{\beta_i}}+1)$. 记 $t_{(g_i)}=2^{(\alpha-1)}\prod_{i=1}^{k}q_i^{\beta_i}/q_i$，

$x^{2^{(\alpha-1)}\prod_{i=1}^{k}q_i^{\beta_i}}+1=(x^{t(q_1)}+1)(\sum_{i=0}^{q_1-1}(-1)^i x^{t(q_1)i})=(x^{t(q_2)}+1)(\sum_{i=0}^{q_2-1}(-1)^i x^{t(q_2)i})=\ldots=(x^{t(q_k)}+1)(\sum_{i=0}^{q_k-1}(-1)^i x^{t(q_k)i})$.

原根不在方程组 $x^{t(q_i)}+1\equiv 0(\mathrm{mod}p)$中，在方程组(Ⅺ)中.

$g_{(x)}=\{x|\sum_{i=0}^{q_i-1}(-1)^i x^{t(q_i)i}\equiv 0(\mathrm{mod}p),i=1,2,\ldots,k\}=\bigcap_{j(p)}(p_{(p)}\cup f_{(p)})$.　　(Ⅺ)　　□

因为 $q_1,q_2,\ldots,q_k$ 两两互质，(Ⅺ)中方程的次数各不相等.由定理 5，用(Ⅺ)来分离(ii)中不含原根的因式，得 $g_{(x)}\equiv 0(\mathrm{mod}p)$.

例 9、求下列数的原根.

（1）17；　（2）211.

解　（1）$\varphi(\varphi(17))=\varphi(16)=8$. $x^{16}-1=(x^8-1)(x^8+1)\equiv 0(\mathrm{mod}17)$.

$j_{(17)}=\{\pm1,\pm2,\ldots,\pm8\}$, $p_{(17)}=\{\pm1,\pm2,\pm4,\pm8\}$, $g_{(17)}=\{\pm3,\pm5,\pm6,\pm8\}$.

（2）$\varphi(210)=\varphi(2)\,\varphi(3)\,\varphi(5)\,\varphi(7)=48$. $x^{210}-1=(x^{105}-1)(x^{105}+1)$.

$x^{105}+1=(x^{35}+1)$(①)$=(x^{21}+1)$ (②)$=(x^{15}+1)$ (③).

①$=x^{70}-x^{35}+1$; ②$=x^{84}-x^{63}+x^{42}-x^{21}+1$; ③$=x^{90}-x^{75}+x^{60}-x^{45}+x^{30}-x^{15}+1$.

①∩②$=x^{56}+x^{49}-x^{35}-x^{28}-x^{21}+x^7+1$.　④

$g_{(x)}=$③∩④$=x^{48}-x^{47}+x^{46}-x^{42}+2x^{41}-x^{40}+x^{39}+x^{36}-x^{35}+x^{34}-x^{33}+x^{32}-x^{31}-x^{28}-x^{26}-x^{24}$
$-x^{22}-x^{20}-x^{17}+x^{16}-x^{15}+x^{14}-x^{13}+x^{12}+x^9-x^8+2x^7-x^6+x^5+x^2-x+1$　⑤.

211 的 48 个原根在 $g_{(x)}\equiv 0(\mathrm{mod}211)$中.

$x^{70}-x^{35}+1=(x^{14}-x^7+1)(x^8+x^7-x^5-x^4-x^3+x+1)$ (⑤), $j_{(211)}=\{\pm1,\pm2,\ldots,\pm105\}$.

$f_{(211)}=\{x|(x^{35}+1)(x^{14}-x^7+1)(x^8+x^7-x^5-x^4-x^3+x+1)\equiv 0(\mathrm{mod}211)\}$.

$p_{(211)}$={1,－2,－3,4,5,6,－7,－8,9,－10,11,－12,13,14,－15,16,－17,－18,19,20,21,－22,
－23,24,25,－26,－27,－28,－29,30,－31,－32,－33,34,－35,36,37,－38,－39,－40,－41,
－42,43,44,45,46,47,－48,49,－50,51,52,53,5455,56,－57,58,59,－60,－61,62,－63,64,65,66,
－67,－68,69,70,71,－72,73,－74,－75,76,－77,78,79,80,81,82，83,84,－85,－86,87,－88,－89, －90,－91,
－92,93,－94,95,96,－97,－98,99,100,101,－102,103,－104,105}.

$\{x|x^{35}+1\equiv 0(\mathrm{mod}211)\}$={－1,－5,8,－11,12,－13,18,23,－25,27,28,40,42,－55,－58,60,63,－64,－65，67,68,
－71,－76,－79,82,86,－87,88,89,90,－96,97,98,102,104}.

$\{x|x^{14}-x^7+1\equiv 0(\mathrm{mod}211)\}$= {－14,15,26,31,32,33,－34,38,－43,50,－54,－73,94,－101}.

$\{x|x^8+x^7-x^5-x^4-x^3+x+1\equiv 0(\mathrm{mod}211)\}$={10,－19,－21,61,74,77,－83,－100}.

$g_{(211)}$= {2,3,－4,－6,7,－9,－16,17,－20,22,－24,29,－30,35,－36,－37,39,41,－44,－45, －46,－47,48,－49,
－51－52,－53,－56,57,－59,－62,－66,－69,－70, 72,75,－78,－80,－81,－84,85,91,92,－93,－95,－99,－
103,－105}.

5.2.原根在因式分解中的应用

设 $f(2t,d_t)=\sum_{i=0}^{2t/d_t}(-1)^i x^{2t-id_t}$.　(Ⅻ)　这里 d_t 为 t 的约数，$(4t+2d_t+1)$是素数.

x 的指数是以 d_t 为公差的等差数列，系数为$(-1)^i$，如果(Ⅻ)的项数是合数，那么(Ⅻ)可分解. 下面讨论(Ⅻ)的项数是奇素数的情况.

d_t 为 t 的约数，x 的指数是以 d_t 为公差的等差数列，d_t 不同，数列的公差不同，(Ⅻ)的项数不同. 记 $T_{(t)}$为 t 约数数目，(Ⅻ)的表达式有 $T_{(t)}$个.

定理 14　设 $P(P=4t+2d_t+1)$是素数，

(i)如果 $\varphi(4t+2d_t)=2t$，那么(Ⅻ)不可分解；

(ii)如果 $\varphi(4t+2d_t)<2t$, 那么(Ⅻ)可分解.

证 (i)　$f(2t,d_t)=\sum_{i=0}^{2t/d_t}(-1)^i x^{2t-id_t}=\dfrac{x^{2t+d_t}+1}{x^{d_t}+1}=\dfrac{x^{4t+2d_t}-1}{(x^{d_t}+1)(x^{2t+d_t}-1)}$.

P 的原根不在方程 $x^{2t+d_t}-1\equiv 0(\mathrm{mod}\ p)$及 $x^{d_t}+1\equiv 0(\mathrm{mod}\ p)$中. 如果(Ⅻ)还可分解，那么(Ⅻ)中原根的数目小于 $2t$. 这与 $\varphi(4t+2d_t)=2t$ 相矛盾. (i)成立.

(ii) $g(x)$为整系数多项式.$\varphi(4t+2d_t)<2t$，(Ⅻ)中存在整系数多项式 $f(x)$，使 $f(2t, d_t)=f(x)g(x)$成立.所以(Ⅻ)可分解. (ii)成立. □

例 10 判别下列各式是否可以分解，可分解的将其分解.

(1) $x^{12}-x^{10}+x^8-x^6+x^4-x^2+1$;　　(2) $x^{804}-x^{603}+x^{402}-x^{201}+1$.

解 (1)　$2(12+2)+1=29$,　$\varphi(28)=12$,　(1)不可分解.

(2)　$2(804+201)+1=2011$, $\varphi(2010)=528<804$，(2)可分解.

$x^{2010}-1=(x^{1005}-1)(x^{1005}+1)$,

$x^{1005}+1=(x^{201}+1)(x^{804}-x^{603}+x^{402}-x^{201}+1)=(x^{335}+1)(x^{670}-x^{335}+1)$.

$x^{804}-x^{603}+x^{402}-x^{201}+1$ 及 $x^{670}-x^{335}+1$ 的公因式为 $x^{536}+x^{469}-x^{335}-x^{268}-x^{201}+x^{67}+1$.

$x^{804}-x^{603}+x^{402}-x^{201}+1=(x^{536}+x^{469}-x^{335}-x^{268}-x^{201}+x^{67}+1)(x^{268}-x^{201}+x^{134}-x^{67}+1)$.

参考文献:

[1] 华罗庚.《数论导引》[M].北京:科学出版社.(1979)

[2]闵嗣鹤　严士健.《初等数论》[M].北京:高等教育出版社.(2003)

[3]熊全淹.《初等数论》[M].武汉:湖北教育出版社.(1982)

[3]宋开福.《初等数论》[M].北京:中国戏剧出版社.(2007)