第四章 二次同余式与平方剩余

4.1 一般二次同余式（三种是变型）

一般形式：$ax^2+bx+c\equiv 0 \pmod m$ $(a\not\equiv 0 \pmod m)$

∵ m 有素因数分解 $m=p_1^{\alpha_1}\cdots p_k^{\alpha_k}$

∴ 一般形式等价于 $\begin{cases} ax^2+bx+c\equiv 0 \pmod{p_1^{\alpha_1}} \\ \vdots \\ ax^2+bx+c\equiv 0 \pmod{p_k^{\alpha_k}} \end{cases}$

∴ 讨论素数幂 p^α 的同余式 $ax^2+bx+c\equiv 0 \pmod{p^\alpha}$ $p\nmid a$

$$4a^2x^2+4abx+4ac\equiv 0 \pmod{p^\alpha}$$

$$(2ax+b)^2\equiv b^2-4ac \pmod{p^\alpha}$$

令 $y=2ax+b$，有

$$y^2\equiv b^2-4ac \pmod{p^\alpha}$$

1. 设 m 是正整数，若 $x^2\equiv a \pmod m$，$(a,m)=1$ 有解，则 a 叫做模 m 的平方（二次）剩余，否则就是平方非剩余。

例1：$x^2\equiv 1 \pmod 4$ 有解 $x\equiv \pm 1 \pmod 4$，故 1 是模 4 平方剩余

$x^2\equiv -1 \pmod 4$ 无整数解，故 -1 是模 4 平方非剩余

$x^2\equiv 1,2,4 \pmod 7$ 有解　因为 $1^2\equiv 1, 2^2\equiv 4, 3^2\equiv 2, 4^2\equiv 2, 5^2\equiv 4, 6^2\equiv 1 \pmod 7$

$x^2\equiv 3,5,6 \pmod 7$ 无解

例2：求满足 $E: y^2=x^3+x+2 \pmod 7$ 的所有点

X 的所有可能解为 $0,1,2,3,4,5,6$

$X=0$，$y^2=2 \pmod 7$，$y\equiv 3,4 \pmod 7$

$X=1$，$y^2=4 \pmod 7$，$y\equiv 2,5 \pmod 7$

$X=2$，$y^2=5 \pmod 7$，无解

$x=3$, $y^2=4 \pmod 7$, $y \equiv 2,5 \pmod 7$

$x=4$, $y^2=0 \pmod 7$, $y \equiv 0 \pmod 7$

$x=5$, $y^2=6 \pmod 7$, 无解

$x=6$, $y^2=0 \pmod 7$, $y \equiv 0 \pmod 7$

共8个点.

例3: 求解 $x^2 \equiv 46 \pmod{105}$

$105=3\times5\times7$

$\therefore$ 等价于 $\begin{cases} x^2 \equiv 46 \equiv 1 \pmod 3 \\ x^2 \equiv 46 \equiv 1 \pmod 5 \\ x^2 \equiv 46 \equiv 4 \pmod 7 \end{cases}$ → 与常规中乘有些许不同

解得 $\begin{cases} x_1 \equiv \pm 1 \pmod 3 \\ x_2 \equiv \pm 1 \pmod 5 \\ x_3 \equiv \pm 2 \pmod 7 \end{cases}$ → $2\times2\times2$, 8种中剩组合, 8个解

$M=3\times5\times7=105$

$\begin{cases} M_1=35 \\ M_2=21 \\ M_3=15 \end{cases}$ $\begin{cases} M_1'=2 \\ M_2'=1 \\ M_3'=1 \end{cases}$

$\therefore x \equiv b_1 \cdot 70 + b_2 \cdot 21 + b_3 \cdot 15 \pmod{105}$

$\therefore x=1\cdot70+1\cdot21+2\cdot15=121=16 \pmod{105}$

$x=1\cdot70+1\cdot21+(-2)\cdot15=61\equiv61 \pmod{105}$

$x=1\cdot70+(-1)\cdot21+2\cdot15=79\equiv79 \pmod{105}$

$\vdots$

$x=(-1)\cdot70+(-1)\cdot21+(-2)\cdot15=-121\equiv89 \pmod{105}$

4.2 模为奇素数的平方剩余与平方非剩余

→ 这是奇素数, 其实素数中也只有2是偶的

4.1 中普通的 $x^2 \equiv a \pmod p$, $(a,p)=1$

1. 判断是否有解

① 设 p 为奇素, $(a,p)=1$

∴ 若 a 是模 p 的平方剩余 $\xrightarrow{充要}$ $a^{\frac{p-1}{2}} \equiv 1 \pmod p$

∴ 非 ~ $\xrightarrow{充要}$ $a^{\frac{p-1}{2}} \equiv -1 \pmod p$

证明：⇒ ∵ p 为奇素

∴ 有 $x^p - x = x\left((x^2)^{\frac{p-1}{2}} - a^{\frac{p-1}{2}}\right) + \left(a^{\frac{p-1}{2}} - 1\right)x$

$= x\,g(x)\cdot(x^2 - a) + \left(a^{\frac{p-1}{2}} - 1\right)x$

若 a 是模 p 的平方剩余，即 $x^2 \equiv a \pmod p$ 有两解，即余式系数被 p 整除，即

$$p \mid a^{\frac{p-1}{2}} - 1$$

3.4：$x^p - x$ 被 $f(x)$ 除得的余式的系数都是 p 的倍数 ⇔ $f(x) = 0$ 有 n 个解

反过来，若 $a^{\frac{p-1}{2}} \equiv 1 \pmod p$，有 $x^2 \equiv a \pmod p$ 有解

⇐ 欧拉：$\left(a^{\frac{p-1}{2}} + 1\right)\left(a^{\frac{p-1}{2}} - 1\right) = a^{p-1} - 1 \equiv 0 \pmod p$

有 $\underbrace{p \mid a^{\frac{p-1}{2}} - 1}_{\text{剩余}}$ 或 $\underbrace{p \mid a^{\frac{p-1}{2}} + 1}_{\text{非剩余}}$

即 $a^{\frac{p-1}{2}} \equiv -1 \pmod p$

例：判断 137 是否为模 227 平方剩余

$137^{\frac{227-1}{2}} = 137^{113}$

$113 = 2^0 + 2^4 + 2^5 + 2^6$

求 $137^{113} \pmod{227}$

$n_0 = 1,\ a_0 = 137,\ b_1 = 137^2 \equiv 155 \pmod{227}$

$n_1 = 0,\ a_1 = a_0 = 137,\ b_2 = b_1^2 = 190 \pmod{227}$

⋮

得 $137^{113} \equiv -1 \pmod{227}$

∴ 137 为模 227 平方非剩余

2. p为奇素，$(a_1,p)=1$，$(a_2,p)=1$，则

① a_1,a_2 都是模p的平方剩余，则 $a_1\cdot a_2$ 也是

② a_1,a_2 ~~~~非~，则 $a_1\cdot a_2$ 是

③ 一个是一个不是，$a_1\cdot a_2$ 不是

证：$(a_1\cdot a_2)^{\frac{p-1}{2}}=a_1^{\frac{p-1}{2}}\cdot a_2^{\frac{p-1}{2}}$，再用证。

3. p是奇素数，则p的简化剩余系中 {平方剩余 各占一半 $\frac{p-1}{2}$ / 平方非剩余

且 $\frac{p-1}{2}$ 个平方剩余与序列 $1^2,2^2,\cdots,(\frac{p-1}{2})^2$ 中的一个数同余且仅与一个。

例：p=7

1 2 3 4 5 6

对应 1, 4, 9

mod 7

1→1

2→9

4→4

一一对应

1: $1^{\frac{7-1}{2}}\equiv 1\pmod 7$ 有解

2: $2^{\frac{7-1}{2}}\equiv 1\pmod 7$ 有

3: $3^{\frac{7-1}{2}}\not\equiv 1\pmod 7$ 无

4: $4^{\frac{7-1}{2}}\equiv 1\pmod 7$ 有

5: $5^{\frac{7-1}{2}}\not\equiv 1\pmod 7$ 无

6: $6^{\frac{7-1}{2}}\not\equiv 1\pmod 7$ 无

$\frac{7-1}{2}=3$ 个一半

证明：由1.得，若是平方剩余，则 $a^{\frac{p-1}{2}}\equiv 1\pmod p$

∴ 个数 = 方程 $x^{\frac{p-1}{2}}\equiv 1\pmod p$ 的解数

但 $x^{\frac{p-1}{2}}-1\mid x^{p-1}-1$，∴解有 $\frac{p-1}{2}$ 个

∴非个数 $=p-1-\frac{p-1}{2}=\frac{p-1}{2}$

$x^{p-1}\equiv 1\pmod p$，多理解

对于 $x^a+1 \mid x^{2a}-1$

证明：$x^{2a}-1=(x^a+1)(x^a-1)$

因此一定可以整除

4.3 勒让得符号

1. 勒让得符号之运算性质

42中给出了判断有二次剩余的法则

$x^2\equiv a \pmod p$，若 $a^{\frac{p-1}{2}}\equiv 1 \pmod p$，则有.

但还是复杂，这里给出一种更简单的判别、计算法则.

① p为素，定义勒让得符号：

$$\left(\frac{a}{p}\right)=\begin{cases}1, & \text{若 } a \text{ 是模 } p \text{ 的平方剩余}\\ -1, & \sim\sim\sim\sim\sim\sim \text{ 非}\sim\\ 0, & \text{若 } p\mid a\end{cases}$$

∴ 对于 $(a,p)=1$ 有 $\left(\frac{a}{p}\right)=1 \Leftrightarrow x^2\equiv a \pmod p$ 有解

$\left(\frac{a}{p}\right)=-1 \Leftrightarrow x^2\equiv a \pmod p$ 无解

例：$\left(\frac{-1}{11}\right)=\left(\frac{1}{11}\right)=\left(\frac{2}{11}\right)=\left(\frac{-5}{11}\right)=\left(\frac{8}{11}\right)=\left(\frac{9}{11}\right)=\left(\frac{-3}{11}\right)=\left(\frac{-15}{11}\right)=1$

$\left(\frac{2}{11}\right)=\left(\frac{5}{11}\right)=\left(\frac{6}{11}\right)=\left(\frac{7}{11}\right)=\left(\frac{10}{11}\right)=\left(\frac{-4}{11}\right)=\left(\frac{-12}{11}\right)=\left(\frac{15}{11}\right)=-1$

② 欧拉判别法则.

p为素，对于任意整 a

有 $\left(\frac{a}{p}\right)\equiv a^{\frac{p-1}{2}} \pmod p$ 太简单，不用证了

③ p为奇素.

1) $\left(\frac{1}{p}\right)=1$

2) $\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}$ 太简单，不用证了

例：$x^2 \equiv -1 \pmod{365}$ 有解？有几个？

$\left(\frac{-1}{365}\right) = (-1)^{\frac{365-1}{2}} = 1 \pmod{365}$ 有解

$365 = 5 \cdot 73$

原式等价于 $\begin{cases} x^2 \equiv -1 \pmod 5 \\ x^2 \equiv -1 \pmod{73} \end{cases}$

$\left(\frac{-1}{5}\right) = (-1)^{\frac{5-1}{2}} = 1$，$\left(\frac{-1}{73}\right) = (-1)^{\frac{73-1}{2}} = 1$

2个　　2个

共4个解

④ 勒让得符号的函数性质：

p为奇素

1) 周期性：$\left(\frac{a+p}{p}\right) = \left(\frac{a}{p}\right)$

2) 完全可乘性：$\left(\frac{a \cdot b}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

3) 设 $(a,p)=1$，则 $\left(\frac{a^2}{p}\right) = 1$ ⟶ 费马定理

⇓ 推论

若 $a \equiv b \pmod p$，则 $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$

2. 高斯引理

高斯(Gauss)给出另一种判断a是否为模p二次剩余的判别方法

① p为奇素，a整，$(a,p)=1$，若

$a \cdot 1, a \cdot 2, a \cdot 3, \cdots, a \cdot \frac{p-1}{2}$

中模p的最小正剩余大于$\frac{p}{2}$的个数是m，则 $\left(\frac{a}{p}\right) = (-1)^m$

② p为奇素

1) $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$　　一般用这个多一些

3) 若 $(a,2p)=1$，则 $\left(\frac{a}{p}\right)=(-1)^{T(a,p)}$，$T(a,p)=\sum_{k=1}^{\frac{p}{2}}\left[\frac{a\cdot k}{p}\right]$ ↓ 取整符号

例1：判断2,3是否为模17的平方剩余.

由3)得 $\left(\frac{2}{17}\right)=(-1)^{\frac{17^2-1}{8}}=(-1)^{2\cdot 18}=1$ 是

由2)得，$(3,34)=1$

$$T(3,17)=\sum_{k=1}^{8}\left[\frac{3k}{17}\right]=3$$

$$\therefore \left(\frac{3}{17}\right)=(-1)^3=-1$$ 不是

例2：假设 $p=8k+5$ 为素数，则2为模p平方非剩余.

证明：$p=8k+5$ 为奇素

法一：$\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}=(-1)^{\frac{(8k+5)^2-1}{8}}=-1$ 非剩余.

法二：$2^{\frac{p-1}{2}}=2^{4k+2}\ \mathrm{mod}(8k+5)$ 不好算，还是要用高斯.

例3：$x^2\equiv 2 \pmod{3599}$ 有解？有几个？

$3599=59\cdot 61$

等价于 $\begin{cases}x^2\equiv 2 \pmod{59}\\ x^2\equiv 2 \pmod{61}\end{cases}$

$\left(\frac{2}{59}\right)=(-1)^{\frac{59^2-1}{8}}=-1$ 无解.

2. 回归性论：$\left(\frac{2}{p}\right)=\begin{cases}1, & p\equiv \pm 1 \pmod 8\\ -1, & p\equiv \pm 3 \pmod 8\end{cases}$

证：$\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}$ ← 算奇偶次行.

4.4 二次互反律

设 p,q 是不同的奇素数，求 $\begin{cases} x^2 \equiv q \pmod p \\ x^2 \equiv p \pmod q \end{cases}$ 之间的联系

1. 定理内容：若 p,q 是不同的奇素数，则

$$\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \left(\frac{p}{q}\right)$$

证：原式等价于 $\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$

$\because (2, pq) = 1$

$\therefore$ 有 $\left(\frac{q}{p}\right) = (-1)^{T(q,p)}$，$\left(\frac{p}{q}\right) = (-1)^{T(p,q)}$

$$T(q,p) = \sum_{h=1}^{\frac{p-1}{2}} \left[\frac{q\cdot h}{p}\right],\quad T(p,q) = \sum_{k=1}^{\frac{q-1}{2}} \left[\frac{p\cdot k}{q}\right]$$

$\therefore$ 证 $T(q,p) + T(p,q) = \frac{p-1}{2}\cdot\frac{q-1}{2}$

书P38看图理解

例1：$x^2 \equiv 137 \pmod{227}$ 有解？

$$\left(\frac{137}{227}\right) = \left(\frac{-90}{227}\right) = \left(\frac{-1}{227}\right)\left(\frac{2\cdot 3^2\cdot 5}{227}\right)$$

$$= \left(\frac{-1}{227}\right)\left(\frac{2}{227}\right)\left(\frac{3^2}{227}\right)\left(\frac{5}{227}\right)$$

$(-1)^{\frac{227-1}{2}} = -1$，$(-1)^{\frac{227^2-1}{8}} = (-1)^{\frac{226\times 226}{8}} = -1$

求 $\left(\frac{5}{227}\right)$

法一：227为素数

$5^{\frac{227-1}{2}} \bmod 227$ 不好求

$\left(\frac{a^2}{p}\right) = (a^2)^{\frac{p-1}{2}} = a^{p-1} \equiv 1 \pmod p$ 费尔马

法二：$(5, 2\times 227) = 1$

$\left(\frac{5}{227}\right) = (-1)^{T(5,227)}$

$T(5,227) = \sum_{k=1}^{\frac{227-1}{2}} \left[\frac{5k}{227}\right]$ 太多了，也不好求

法三：$\left(\frac{5}{221}\right)=(-1)^{\frac{221-1}{2}\cdot\frac{5-1}{2}}\left(\frac{221}{5}\right)=\left(\frac{2}{5}\right)=(-1)^{\frac{5^2-1}{8}}=-1$

$\left(\frac{q}{p}\right)=\left(\frac{a+p}{p}\right)$

例2：素数 $p=2000\cdots0029967\approx 2^{100}\approx 10^{30}$，$q=41$，$x^2\equiv q \pmod p$ 有解？

p,q 为素

$\left(\frac{q}{p}\right)=(-1)^{\frac{q-1}{2}\cdot\frac{p-1}{2}}\left(\frac{p}{q}\right)=\left(\frac{-2}{41}\right)=1$

偶

1

$\left(\frac{10^{30}}{41}\right)=\left(\frac{10}{41}\right)^{30}=1$

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

$\therefore \left(\frac{q}{p}\right)=1$，有解

难点：$\left(\frac{p}{q}\right)$ 怎么化简

$(2\times 10^{10}+29967)\pmod{41}$

用前面的知识：

$10^{10}\pmod{41}\equiv 18^5\pmod{41}$ 死算吧，也不费事

$29967\pmod{41}$ 也是死算，不费事

例3：素数 $p=2^{192}-2^{64}-1$，$q=79$，$x^2\equiv q \pmod p$ 有解？

$\left(\frac{q}{p}\right)=(-1)^{\frac{q-1}{2}\cdot\frac{p-1}{2}}\left(\frac{p}{q}\right)=-\left(\frac{p}{q}\right)$

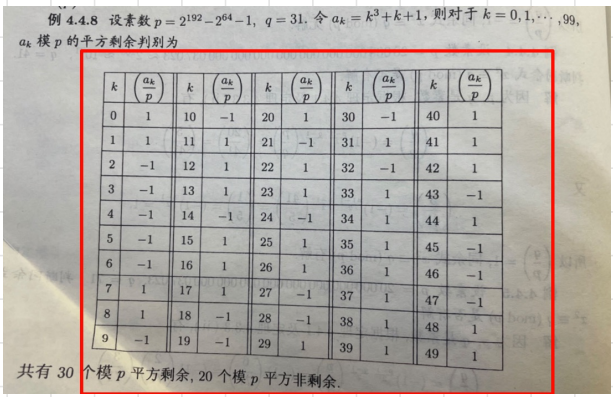
$(2^{192}-2^{64}-1)\pmod{79}$

又 $\because 2^{78}\equiv 1 \pmod{79}$

$\therefore (2^{36}-2^{64}-1)\pmod{79}$ 死算也不费事

例4：素数 $p=2^{192}-2^{64}-1$，$q=31$，令 $a_k=k^3+k+1$，则对于 $k=0,1,\cdots,99$，a_k 模 p 的平方剩余判别为？

$$\left(\frac{a_k}{p}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{a_k-1}{2}}\left(\frac{p}{a_k}\right)$$



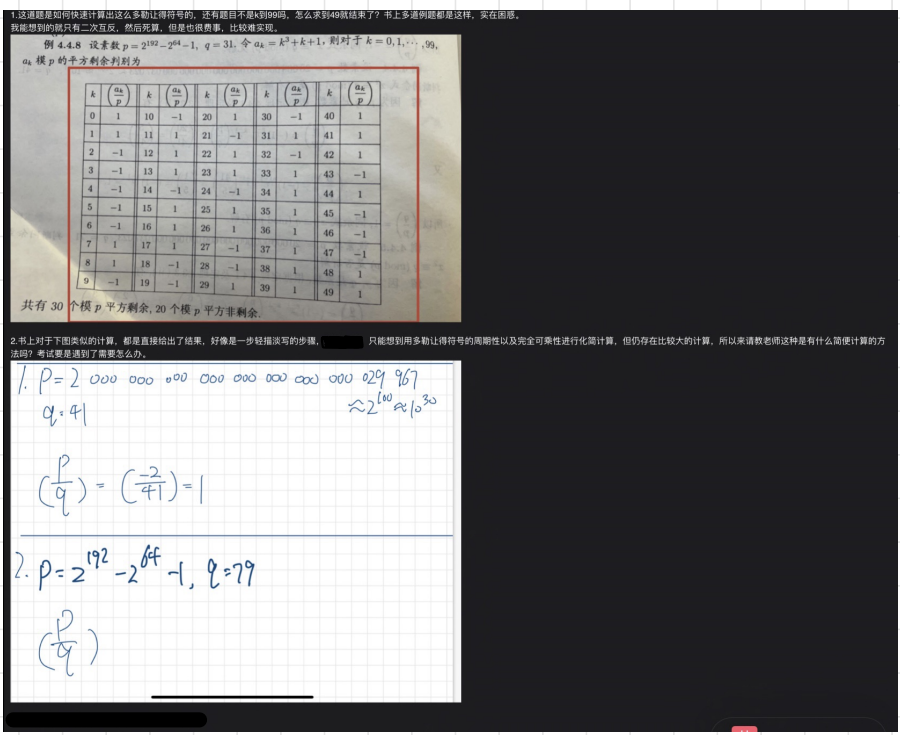
例 4.4.8 设素数 $p=2^{192}-2^{64}-1$，$q=31$. 令 $a_k=k^3+k+1$，则对于 $k=0,1,\cdots,99$，a_k 模 p 的平方剩余判别为

k	$\left(\frac{a_k}{p}\right)$	k	$\left(\frac{a_k}{p}\right)$	k	$\left(\frac{a_k}{p}\right)$	k	$\left(\frac{a_k}{p}\right)$	k	$\left(\frac{a_k}{p}\right)$
0	1	10	−1	20	1	30	−1	40	1
1	1	11	1	21	−1	31	1	41	1
2	−1	12	1	22	1	32	−1	42	1
3	−1	13	1	23	1	33	1	43	−1
4	−1	14	−1	24	−1	34	1	44	1
5	−1	15	1	25	1	35	1	45	−1
6	−1	16	1	26	1	36	1	46	−1
7	1	17	1	27	−1	37	1	47	−1
8	1	18	−1	28	−1	38	1	48	1
9	−1	19	−1	29	1	39	1	49	1

共有 30 个模 p 平方剩余，20 个模 p 平方非剩余.

这道题是如何快速计算出这么多勒让得符号的，还有题目不是k到99吗，怎么求到49就结束了？书上多道例题都是这样，实在困惑。

问老师了，等着吧。



1.这道题是如何快速计算出这么多勒让得符号的，还有题目不是k到99吗，怎么求到49就结束了？书上多道例题都是这样，实在困惑。
我能想到的就只有二次互反，然后死算，但是也很费事，比较难实现。

例 4.4.8 设素数 $p=2^{192}-2^{64}-1$，$q=31$. 令 $a_k=k^3+k+1$，则对于 $k=0,1,\cdots,99$，a_k 模 p 的平方剩余判别为

k	$\left(\frac{a_k}{p}\right)$	k	$\left(\frac{a_k}{p}\right)$	k	$\left(\frac{a_k}{p}\right)$	k	$\left(\frac{a_k}{p}\right)$	k	$\left(\frac{a_k}{p}\right)$
0	1	10	−1	20	1	30	−1	40	1
1	1	11	1	21	−1	31	1	41	1
2	−1	12	1	22	1	32	−1	42	1
3	−1	13	1	23	1	33	1	43	−1
4	−1	14	−1	24	−1	34	1	44	1
5	−1	15	1	25	1	35	1	45	−1
6	−1	16	1	26	1	36	1	46	−1
7	1	17	1	27	−1	37	1	47	−1
8	1	18	−1	28	−1	38	1	48	1
9	−1	19	−1	29	1	39	1	49	1

共有 30 个模 p 平方剩余，20 个模 p 平方非剩余.

2.书上对于下图类似的计算，都是直接给出了结果，好像是一步轻描淡写的步骤，[redacted]只能想到用多勒让得符号的周期性以及完全可乘性进行化简计算，但仍存在比较大的计算，所以来请教老师这种是有什么简便计算的方法吗？考试要是遇到了需要怎么办。

1. $p=2\,000\,000\,000\,000\,000\,000\,000\,000\,000\,029\,967$，$\approx 2^{100}\approx 10^{30}$

$q=41$

$\left(\frac{p}{q}\right)=\left(\frac{-2}{41}\right)=1$

2. $p=2^{192}-2^{64}-1$，$q=79$

$\left(\frac{p}{q}\right)$

解答

勒让得符号的计算确实是使用二次互反定理和基本的一些勒让得符号值得到的。就你提出的问题，可以从以下角度考虑：
1. 书中例4.4.8的题目有些问题，可以理解为刊印错误，应该都是k从0至49; 而且 q=31 也是多余的。至于每个a_k, 相应的勒让得符号计算，可以参考例4.4.6，当 q=79时，由于 2^{64}=-28 mod 79 (方幂模运算)，进而 p=28(1-28^2)-1 mod 79 = 28(1-38*4)-1 = 28*7-1=38-1=37 mod 79 。
这样结合一些方幂模运算和同余的性质，可以简化计算。当然，对于一般的情况，只能利用计算机软件辅助实现了。正常情况下，不会人工计算特别大的数值。
2. 对于10^{30}左右规模的计算，一般通过带余除法求，人工计算没有太多技巧。或者也是通过计算机软件辅助实现。
总之，考察时主要看原理。不会出现上述类似太大的计算量。

例5. 求所有奇素数 p 以3为其二次剩余.

$$\left(\frac{3}{p}\right)=1$$

① 当 $p=3$ $\left(\frac{3}{3}\right)$ $3^{\frac{3-1}{2}}\equiv 0 \pmod 3$ 不成立.

② 当 $p>3$

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

$$\therefore (-1)^{\frac{p-1}{2}}=\begin{cases}1, & \text{当 } p\equiv 1 \pmod 4\\ -1, & \text{当 } p\equiv -1 \pmod 4\end{cases}$$

联合用中国剩余

$$\text{2)}\ \left(\frac{p}{3}\right)=\begin{cases}\left(\frac{1}{3}\right)=1, & \text{当 } p\equiv 1 \pmod 3\\ \left(\frac{-1}{3}\right)=-1, & \text{当 } p\equiv -1 \pmod 3\end{cases}$$

1, 4, 7, 10 都不行.

细节: p 为大于3的奇素数!

$$\therefore \left(\frac{p}{3}\right)=\begin{cases}\left(\frac{1}{3}\right)=1, & \text{当 } p\equiv 1 \pmod 6\\ \left(\frac{-1}{3}\right)=-1, & \text{当 } p\equiv -1 \pmod 6\end{cases}$$

$$\therefore \text{有}\begin{cases}p\equiv 1 \pmod 4\\ p\equiv 1 \pmod 6\end{cases}\ \text{或}\ \begin{cases}p\equiv -1 \pmod 4\\ p\equiv -1 \pmod 6\end{cases}$$

$$\Downarrow \qquad \Downarrow$$

$$p\equiv 1 \pmod{12} \qquad p\equiv -1 \pmod{12}$$

解普通一元线性同余方程组:

① 中国剩余定理 (素)

② 两两相消

$$\begin{cases}p\equiv 1 \pmod 4\\ p\equiv 1 \pmod 6\end{cases}$$

$\Downarrow\Downarrow$

$$\begin{cases} p+4k_1=1 \\ p+6k_2=1 \end{cases}$$

$\therefore 1-4k_1=1-6k_2$

$\therefore 4k_1-6k_2=0 \iff m_1k_1-m_2k_2=a_1-a_2$

有 $gcd(m_1,m_2) \mid (a_1-a_2)$ 解决这个，第三章课后题知识

4.5 雅可比符号

勒让得符号要求模 p 为素数

二次互反律中 p,q 也为奇素数

雅可比目的是弱化这些条件

1. 定义：设 $m=p_1\cdots p_r$ 是奇素数 p_i 的乘积，对于任意整 a，

定义雅可比符号为：$\left(\frac{a}{m}\right)=\left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_r}\right)$

对于 $(a,m)=1$，有：$\left(\frac{a}{m}\right)=1 \Longleftarrow x^2\equiv a \pmod m$ 有解

$\left(\frac{a}{m}\right)=-1 \Longrightarrow x^2\equiv a \pmod m$ 无解

例：3是模119非 $\sim$

但 $\left(\frac{3}{119}\right)=\left(\frac{-3}{7}\right)\left(\frac{3}{17}\right)=(-1)(-1)=1$

2. 基本运算性质

① $\left(\frac{a+m}{m}\right)=\left(\frac{a}{m}\right)$

② $\left(\frac{ab}{m}\right)=\left(\frac{a}{m}\right)\left(\frac{b}{m}\right)$

③ $(a,m)=1$，则 $\left(\frac{a^2}{m}\right)=1$

3. 其他用于化简的性质

① $m=p_1p_2\cdots p_r$ 是奇数，则

$$\frac{m-1}{2}\equiv\frac{p_1-1}{2}+\cdots+\frac{p_r-1}{2} \pmod 2$$

$\frac{m^2-1}{8} \equiv \frac{p_1^2-1}{8} + \cdots + \frac{p_s^2-1}{8} \pmod 2$

证明: $m \equiv (1+2\cdot\frac{p_1-1}{2})\cdots(1+2\cdot\frac{p_r-1}{2})$

只要有超过两项 $(2\cdot\frac{p_i-1}{2})$ 就是4的倍数

$\equiv 1 + 2\cdot(\frac{p_1-1}{2}+\cdots+\frac{p_s-1}{2}) \pmod 4$

$\therefore \frac{m-1}{2} \equiv \frac{p_1-1}{2}+\cdots+\frac{p_s-1}{2} \pmod 2$

同理有 m^2.

② m 是奇数

用上面定理证

① $(\frac{1}{m})=1$

② $(\frac{-1}{m}) = (-1)^{\frac{m-1}{2}}$

③ $(\frac{2}{m}) \equiv (-1)^{\frac{m^2-1}{8}}$

③ $(\frac{n}{m}) = (-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}}(\frac{m}{n})$

例: $x^2 \equiv 286 \pmod{563}$ 有解?

$$\left(\frac{286}{563}\right) = \left(\frac{2}{563}\right)\left(\frac{143}{563}\right) = (-1)^{\frac{563^2-1}{8}}(-1)^{\frac{563-1}{2}\cdot\frac{143-1}{2}}\left(\frac{563}{143}\right)$$

$$= \left(\frac{-9}{143}\right) = -\left(\frac{3^2}{143}\right) = -1$$

雅可比 $=-1 \Rightarrow$ 无解

$=1 \Leftarrow$ 有解

4.6 模平方根

1. 模 p 平方根.

设 p 是形为 $4k+3$ 的素数.

若 $x^2 \equiv a \pmod p$ 有解, 则其解

$x \equiv \pm a^{\frac{p+1}{4}} \pmod p$ 不能判断是否有解!

证：$\because p=4k+3$ 素

$\therefore$ 有奇数 q，使得 $p-1=2q$

$\therefore x^2\equiv a \pmod p$ 有解，则有

$$a^{\frac{p-1}{2}}\equiv 1 \pmod p$$

$$a^{q}\equiv 1 \pmod p$$

两边同乘 a，得 $\left(a^{\frac{q+1}{2}}\right)^2\equiv a^{q+1}\equiv a \pmod p$

得到

例：素数 $p=2^{192}-2^{64}-1$，$q=79$

$x^2\equiv 9 \pmod p$ 有解？

形为 $4k+3$ 的素数！

$\left(\frac{q}{p}\right)$ 判断仍有解至.

$$x\equiv \pm 79^{\frac{2^{192}-2^{64}}{4}}\equiv \pm 79^{2^{190}-2^{62}} \pmod p$$

2. 模 p 平方根

在有解情况下，考虑二次同余式的具体求解.

① p 为奇素，$p-1=2^t\cdot s$，$t\geq 1$，s 为奇整.

设 n 是模 p 平方非剩余，$b:\equiv n^s \pmod p$ → 定义的意义

若 $x^2\equiv a \pmod p$ 有解，记

$a^{-1}x^2$ 满足同余式 $y^{2^{t-k-1}}\equiv 1 \pmod p$，$k=0,1,\cdots,t-1$

⋮

停. 不看了. 摆 ✗ 比较重要，得看！

例：求解 $x^2\equiv 186 \pmod{401}$

$186=2\cdot 3\cdot 31$

$\left(\frac{186}{401}\right)=\left(\frac{2}{401}\right)\left(\frac{3}{401}\right)\left(\frac{31}{401}\right)=1\cdot(-1)\cdot(-1)=1$，有解

求解看P152.

P奇素. $p-1=2^t \cdot \underbrace{s}_{\text{奇整}}$, $t\geq 1$, n是P平方剩余.

$b:=n^s \pmod p$

若 $x^2\equiv a \pmod p$ 有解, 则 $a^{-1}x_{t-k-1}^2$ 满足

$$y^{2^{t+k-1}} \equiv 1 \pmod p,\ k=0,1,\cdots,t-1$$

$$x_{t-1}:=a^{\frac{s+1}{2}} \pmod p$$

$$x_{t-k-1}=x_{t-k}\,b^{j_{k-1}2^{k-1}}$$

$$j_{k-1}=\begin{cases}0, & \text{若 } (a^{-1}x_{t-k}^2)^{2^{t-k-1}}\equiv 1 \pmod p\\ 1, & \text{若 } (a^{-1}x_{t-k}^2)^{2^{t-k-1}}\equiv -1 \pmod p\end{cases}$$

用数学归纳法证明.

3. 模m平方根.

讨论m为合数的二次同余式.

$$x^2\equiv a \pmod m,\quad (a,m)=1$$

$$m=2^{\delta}p_1^{\alpha_1}\cdots p_k^{\alpha_k} \Leftrightarrow \begin{cases}x^2\equiv a \pmod{2^{\delta}}\\ x^2\equiv a \pmod{p_1^{\alpha_1}}\\ \vdots\\ x^2\equiv a \pmod{p_k^{\alpha_k}}\end{cases}$$

(1) 讨论 $x^2\equiv a \pmod{p^{\alpha}}$, $(a,p)=1$, $a>0$

有解 $\underset{\text{要}}{\overset{\text{充}}{\Longleftrightarrow}}$ a为模P平方剩余

且有解时, 解数为2.

证明: 设有解, 则有 $x\equiv x_1 \pmod{p^{\alpha}}$ 使 $x_1^2\equiv a \pmod{p^{\alpha}}$

则有 $x_1^2\equiv a \pmod p$

② p为奇素，对于任意整数a，$x^2\equiv a \pmod{p^\alpha}$解数是

$T=1+\left(\frac{a}{p}\right)$

证：1）当$\left(\frac{a}{p}\right)=0$时，$x^2\equiv a\equiv 0 \pmod p$有唯一解$x\equiv 0 \pmod p$

满足$T=1+\left(\frac{a}{p}\right)$

2）$\left(\frac{a}{p}\right)=1$，$x^2\equiv a \pmod p$有2，满足$T=1+\left(\frac{a}{p}\right)$

3）$\left(\frac{a}{p}\right)=-1$，$x^2\equiv a \pmod p$无解，满足$T=1+\left(\frac{a}{p}\right)$

③ 设$\alpha>1$，$x^2\equiv a \pmod{p^\alpha}$有解必要条件是

1）当$\alpha=2$时，$a\equiv 1 \pmod 4$

2）当$\alpha\geq 3$时，$a\equiv 1 \pmod 8$

4.7 $x^2+y^2=p$

$x^2+y^2=p$有解 $\overset{\text{充要}}{\Longleftrightarrow}$ $p=2$或$4k+1$为模p平方剩余

（$p=2$或$p=4k+1$）