~~3. 求解模p平方根.~~

△信息论数学基础：例题汇总.

1. 最大公因数辗转相除 (1020, 225)
2. 求(120, 150, 210, 35)
3. 求 $7x+4y=100$ 全解
4. 求 $3^{1000000} \pmod 7$.
5. 求 $\varphi(m)$. $\varphi(2020)$ $\varphi(2011)$.
6. 求 $12996^{227} \pmod{37809}$.
7. 求 $8\cdot9\cdot10\cdot11\cdot12\cdot13 \pmod 7$
8. 求：$33x \equiv 22 \pmod{77}$
9. 求 $\begin{cases} x \equiv 2 \pmod 9 \\ 3x \equiv 4 \pmod 5 \\ 4x \equiv 3 \pmod 7 \end{cases}$
10. 求 $f(x)=x^4+x^3+1=0 \pmod{125}$.
11. 求判断 $2x^3+5x^2+0x+1=0 \pmod 7$ 是否有3个解.
12. 求：$3x^{14}+4x^{13}+2x^{11}+x^8+x^6+x^3+12x^2+x \equiv 0 \pmod 5$
13. 求 模13的平方剩余和平方非剩余
14. 求解 $G: y^2=x^3+x+1 \pmod 7$ 点集有多少个 $(x,y)$
15. 求 $x^2 \equiv 46 \pmod{101}$.
16. 求解 $x^2 \equiv 41 \pmod{64}$.
17. 求 $\left(\frac{151}{373}\right)$.

18. 求所有系数p使得x为模p二次剩余.

19. 求 $2^{1000000} \pmod{77}$. {解一 解二.

20. 高次同余式计算公式.

21. RSA算法.

~~$ed \equiv 1 \pmod{\varphi(n)}$.~~

~~[illegible]~~

~~[illegible]~~

22. 逐步求解注意点:

① 模重复平方: 求 $b^n \pmod m$

令n为二进制 $n = a_0 \cdot 2^0 + a_1 \cdot 2^1 + a_2 \cdot 2^2 + \cdots + a_s 2^s$, $a_i = 1$

A. $a_0 = n_0$: $a_0 = a \cdot b^{n_0} \pmod m$; $b_1 \equiv b^2 \pmod m$

B. $n_0 = n_1$; $a_1 = a_0 \cdot b_1^{n_0} \pmod m$ $b_2 \equiv b_1^2 \pmod m$

...

$\Rightarrow$ S: $n_s = n_s$; $a_s \equiv a_{s-1} \cdot b_s^{n_0} \pmod m \Rightarrow a_s$ 即为最终答案.

② 高次同余式. $f(x) \equiv 0 \pmod{p^\alpha}$. $f(x)$ ~~[illegible]~~

A. 先求 $f(x) \equiv 0 \pmod p$ 特解 $x_1$; $\Rightarrow x_2 = x_1 + pt_1$ $\Rightarrow x_3 = x_2 + p^2 t_2$

B. $\alpha = 2$, 求 $f(x) \equiv 0 \pmod{p^2}$: $\Rightarrow f(x_2) + f'(x_2) \cdot p \cdot t_2 \equiv 0 \pmod{p^2} \Rightarrow t_1$ ✓

C. $\alpha = 3$, 求 $f(x) \equiv 0 \pmod{p^3}$. $\Rightarrow f(x_3) + f'(x_3) p^2 \cdot t_2 \equiv 0 \pmod{p^3} \Rightarrow x_4 = x_3 + p^3 t_3$

...

D. $\alpha$ 时. $f(x_\alpha) + f'(x_\alpha) \cdot p^{\alpha-1} \cdot t_{\alpha-1} \equiv 0 \pmod{p^\alpha} \Rightarrow x_\alpha = x_{\alpha-1} + p^{\alpha-1} \cdot t_{\alpha-1}$. ✓

③ 模 $2^\alpha$ 同余式. $x^2 \equiv a \pmod{2^\alpha}$.

{ $\alpha = 2$. 若 $a \equiv 1 \pmod{2^2} \Rightarrow$ 2解
  $\alpha \geq 3$. 若 $a \equiv 1 \pmod{2^\alpha} \Rightarrow$ 4解

~~A. 特点~~

A. $\alpha = 3$ 时. $x_3 \equiv \pm(1 \pm 4t_3) \pmod 8$

B. $\alpha = 4$ 时. $t_3 = \frac{a - x_3^2}{2^3} \pmod 2 \Rightarrow x_4 = x_3 + 2^3 \cdot t_4$

C. $\alpha = 5$ 时. $t_4 = \frac{a - x_4^2}{2^4} \pmod 2 \Rightarrow x_5 = x_4 + 2^4 \cdot t_5$.

...

$\alpha$ 时. $t_{\alpha-1} = \frac{a - x_{\alpha-1}^2}{2^{\alpha-1}} \pmod 2 \Rightarrow x_\alpha = x_{\alpha-1} + 2^{\alpha-1} \cdot t$. ✓

○信息安全数学基础. 例题汇总

23. 求. 2, 5, 10. 模13的指数

24. 求模13所有原根

25. 求模41所有原根

26. 求模23一个原根指标表. 并据此求 $X^3 \equiv 41 \pmod{23}$

27. 验证341是基于6=2的拟素数 (拟素数. 强拟素数. 欧拉拟素数)

28. 验证561是基于6=2的拟素数

29. 证群. 半群.

30. 证同态. 同构.

31. 变换群. 置换群. 循环置换写法:

$\begin{pmatrix} 1&2&3&4&5 \\ 2&3&1&4&5 \end{pmatrix}$ $\begin{pmatrix} 1&2&3&4&5 \\ 2&1&4&3&5 \end{pmatrix}$

32. 对称群

33. 判断题. 同余式有解. $X^8 \equiv 23 \pmod{41}$ $\text{ind}\,23 = 36$

$X^{12} \equiv 37 \pmod{41}$ $\text{ind}\,37 = 32$.

$(d, \varphi(m)) \mid \text{ind}\,a$ 有解. (允等余体)