P2.23

(a) Find a square root of 340 modulo 437

$(437 = 19 \cdot 23)$

$b^2 \equiv a^{(p+1)/2} \pmod{p}$

$b^2 \equiv 340 \bmod 23$

$340 - (23 \times 14) = 18$

$x_2^2 \equiv 18 \bmod 23$

$4^2 \equiv 16$

$5^2 \equiv 2$

$6^2 \equiv 13$

$7^2 \equiv 3$

$8^2 \equiv 18$ ✓

$15^2 \equiv 18$ ✓

$x_2 = 8, 15$

$x \equiv 13 \bmod 19, x \equiv 8 \bmod 23$

$x \equiv 13 \bmod 19, x \equiv 15 \bmod 23$

$x \equiv 6 \bmod 19, x \equiv 8 \bmod 23$

$x \equiv 6 \bmod 19, x \equiv 15 \bmod 23$

$19y + 6 \equiv 8 \bmod 23$

$19y \equiv 2 \bmod 23$

$19^{-1} \equiv 17 \bmod 23$

$y \equiv 2 \times 17 \equiv 11 \bmod 23$

$x = 19 \times 11 = 215$

$19y + 13 \equiv 15 \bmod 23$

$-13 \quad -13$

$19y \equiv 2 \bmod 23$

$y = 17 \times 2 \bmod 23 = 11 \bmod 23$

$x = 19(11) + 13 = 222$

$b^2 \equiv 340 \bmod 19$

$340 - (17 \times 19) = 17$

$x_1^2 \equiv 17 \bmod 19$

$6^2 \equiv 17 \bmod 19$ ✓

$9^2 \equiv 81 \equiv 5$ ✗

$10^2 \equiv 5$ ✗

$11^2 \equiv 7$ ✗

$12^2 \equiv 11$ ✗

$13^2 \equiv 17$ ✓

$x = 13 \bmod 19$

$x_1 = 13, 6$

$x = 19y + 13$

$19y + 13 = 8 \bmod 23$

$19y = -5 \equiv 18 \bmod 23$

$19y^{-1} \equiv 17 \bmod 23$

$y \equiv 306 \equiv 7 \bmod 23$

$x = 19(7) + 13 = 146$

$x = 19y + 6 \equiv 15 \bmod 23$

$-6 \quad -6$

$19y \equiv 9 \bmod 23$

$y = 9 \times 17 \equiv 15$

$x = 19(15) + 6 \equiv 291$

$x = 146, 215, 222, 291$

2. Solve $3^x \equiv 14 \bmod 31$

$p-1 = 30$, $30 \equiv 2 \cdot 3 \cdot 5$

Suppose $3^x \equiv 14 \bmod 31$ let $q = 2$

$\frac{p-1}{q} = \frac{31-1}{2} = 15$ AND compute $14^{15} \equiv 1 \bmod 31$

$14^2 \equiv 10 \bmod 31$
$14^4 \equiv 7 \bmod 31$
$14^8 \equiv 18 \bmod 31$
$14^{15} = 30 \bmod 31$ $3^{15} \equiv 30 \bmod 31$

$x \equiv 1 \bmod 2$

$q = 3$, $30/3 = 10$, $14^{10} \equiv 1 \bmod 31$

$14^5 = (14^4 \times 14) \bmod 31$

$7 \times 14 = 98 \equiv 5 \bmod 31$
$14^{10} \equiv 25 \bmod 31$
$3^{10} \equiv 25 \bmod 31$

$25^x \equiv 25$, $\underline{x \equiv 1 \bmod 3}$

$q = 5$, $30/5 = 6$, $14^6 \equiv 1 \bmod 31$

$14^6 \equiv 8 \bmod 31$
$3^6 \equiv 16 \bmod 31$

$(3^6)^x = 14^6$

$16^x \equiv 8 \bmod 31$
$\underline{x = 2 \bmod 5}$

CRT - $x \equiv 1 \bmod 2$
$x \equiv 1 \bmod 3$
$x \equiv 2 \bmod 5$

$x = 6(5n+1) + 1$
$x = 30n + 7$

$x = 6y + 1 \equiv 2 \bmod 5$
$6y = 1 \bmod 5$
$y \equiv 1 \bmod 5$
$y = 5n + 1$

$x \equiv 7 \bmod 30$

3. $156^x \equiv 28 \bmod 197$ (g, h, p) — 156 order 49

$q^e = 7^2$

(1-2) x_0 | Raise DLP to $q^{e-1} = 7^1$ power

$b \equiv g^{q^{e-1}}$

$b \equiv 156^{7^1}$

$(156^{7^1})^{x_0} \equiv 28^{7^1} \pmod{197}$

$191^{x_0} \equiv 178 \pmod{197}$

$\rightarrow x_0 = 3 \bmod 7 \rightarrow x = 3 + \ldots$

(3) x_1 | $191^{x_1} \equiv (28 \cdot 156^{-3})^{7^0} \pmod{197}$

$191^{x_1} \equiv (28 \cdot 24^3)^1 \equiv 164$ $\quad 156^{-1} \equiv 24$

$\rightarrow 191^{x_1} \equiv 164 \bmod 197$

$x_1 = 6 \bmod 7 \rightarrow x = 3 + 6 \cdot 7 + \ldots$

(4) x_2 | $191^{x_2} \equiv (28 \cdot 24^{-17})^{7^{-1}}$? No, stop

Answer |

$x = 3 + 6 \cdot 7 = 45$

4 2.28 $g^x = a$ in $\mathbb{F}_p$ 7 is primitive

(a) $p = 433, g = 7, a = 166$

$7^x \equiv 166 \bmod 433$ Find $\mathbb{F}_{433}^*$, $432 = 2^4 \times 3^3$

$x = x_0 + x_1 \cdot 3 + x_2 \cdot 3^2, x_i \in \{0,1,2\}$

b=374 $(7^{24})^{x_0} \equiv 166^{24} \bmod 433$

$374^{x_0} \equiv 335 \bmod 433$

$x_0 = 20 \bmod 27, x_0 = 20$

$(7^{3^3})^{x_1} \equiv 166^{3^3} \bmod 433$

$265^{x_1} \equiv 250 \bmod 433$

$x_1 = 15 \bmod 16$

$x = 27n + 20 \equiv 15 \bmod 16$

$27 \equiv -5 \bmod 16, -5 \equiv 11 \bmod 16$

$11n \equiv 11 \bmod 16, 11^{-1} \equiv 3 \bmod 16$

$n \equiv 33 \equiv 1 \bmod 16$

Plug back in

$x = 27(1) + 20 \equiv 47 \bmod 432$

$x = 47$

5. 3.1 Euler's Theorem and Roots Modulo pq

(a) $x^{19} \equiv 36 \mod 97$

(b) $x^{137} \equiv 428 \mod 541$

(a) $x^{19} \equiv 36 \mod 97$

$96 = (19 \times 5) + 1$

$19^{-1} \equiv -5 \equiv 91 \mod 96$

$d = 91$

$x \equiv 36^{91} \equiv 36 \pmod{97}$

(b) $x^{137} \equiv 428 \mod 541$

$540 = (137 \times 3) + 129$

$137 = (129 \times 1) + 8$

$129 = (8 \times 16) + 1$

$129 = 540 - (137 \times 3)$

$1 = 129 - 16(8)$

$8 = 137 - (129 \times 1)$

$1 = 129 - 16(137 - (129(1))$

$1 = 129 - 16(137) + 129(16)$

$1 = 129(17) - 16(137)$

$1 = (540 - 137(3))(17) - 16(137)$

$540(17) - 137(51) - 16(137)$

$137^{-1} \equiv -67 \equiv 473 \mod 540$

$d = 473$

FIND

$x \equiv 428^{473} \mod 541$

$x \equiv 213 \mod 541$