P2.17

(a) $11^x = 21$ in $\mathbb{F}_{71}$

↳ $11^x = 21 \bmod 71$

1st - $n = 1 + \lfloor \sqrt{N} \rfloor$, $N = 70 \rightarrow n = 1 + \lfloor \sqrt{70} \rfloor = 9$

2nd

Baby Steps

$11^j \bmod 71$

$11^0 \equiv 1 \bmod 71$
$11^1 \equiv 11 \bmod 71$
$11^2 \equiv 50 \bmod 71$
$11^3 \equiv 53 \bmod 71$
$11^4 \equiv 15 \bmod 71$
$11^5 \equiv 23 \bmod 71$
$11^6 \equiv 40 \bmod 71$
$11^7 \equiv 14 \bmod 71$
$11^8 \equiv 12 \bmod 71$

$j = 1 \quad i = 4$

$x = 4 \cdot 9 + 1 = 37$

$x = 37$

Giant Step

Now $11^{-9} = (11^9)^{(-1)} \equiv 61 \bmod 71$

$1 = 7(61) - 6(71)$

$61^{-1} \equiv 7 \bmod 71$

$11^{-9} \equiv 7 \bmod 71$

i
$21 \cdot 7^0 \equiv 21 \bmod 71$
$21 \cdot 7^1 \equiv 5 \bmod 71$
$21 \cdot 7^2 \equiv 35 \bmod 71$
$21 \cdot 7^3 \equiv 32 \bmod 71$
$21 \cdot 7^4 \equiv 11 \bmod 71$
$21 \cdot 7^5 \equiv 6 \bmod 71$
$21 \cdot 7^6 \equiv 42 \bmod 71$
$21 \cdot 7^7 \equiv 10 \bmod 71$
$21 \cdot 7^8 \equiv 70 \bmod 71$

(b) $156^x = 116$ in F_{593}.

$n = 1 + \lfloor \sqrt{N} \rfloor \rightarrow 1 + (12.17) = 13$

BABY STEPS GIANT STEPS [ON WOLFRAM ALPHA]

k	$156^k \bmod 593$
0	1
1	156
2	23
3	30
4	529
5	97
6	307
7	452
8	538
9	315
10	514
11	129
12	555
13	2

← $j = 3$

k	$(116 \cdot 287^k) \bmod 593$
0	116
1	84
2	388
3	465
4	30
5	308
6	39
7	519
8	110
9	141
10	143
11	124
12	8
13	517

← $i = 4$

$287^x = 3 + 4(14)$

$\rightarrow x = 59$

$156^{-14} \bmod 593$

$\rightarrow 156^{-14} = (156^{14})^{-1} \bmod 593$

$\rightarrow 156^{14} \equiv 2 \cdot 156 \equiv 312 \bmod 593$

$312\mu + 593\mu = 1$

$593 = 312(1) + 281$
$312 = 281(1) + 31$
$281 = 31(9) + 2$
$31 = 2(15) + 1$ ← GCD
$2 = 1(2) + 0$

$281 = 593 - 312(1)$
$31 = 312 - [593 - 312(1)]$
$31 = 312(2) - 593(1)$
$2 = [593 - 312(1)] - [312(2) - 593(1)]9$
$2 = 593 - 312(1) - 312(18) + 593(9)$
$2 = 593(10) - 312(19$
$1 = [312(2) - 593(1)] - [593(10) - 312(19)]15$
$1 = 312(2) - 593(1) - 593(150) + 312(285)$
$1 = 312(287) + 593(151)$

$156^{-14} \equiv 287 \bmod 593$

$312^{-1} \equiv 287 \bmod 593$

GIANT STEP

$116 \cdot 287^{\circ} \equiv \quad \bmod 593$

2.18

(a) $x \equiv 3 \bmod 7$

$x \equiv 4 \bmod 9$

$x = 7(y) + 3 \rightarrow 7y + 3 \equiv 4 \bmod 9$

$-3 \quad -3$

$7y \equiv 1 \bmod 9$

$7^{-1} \equiv 1 \bmod 9$

$9 = 7(1) + 2$

$7 = 2(3) + 1$

$2 = 1(2) + 0$

$2 = 9 - 7(1)$

$1 = 7 - [9 - 7(1)](3)$

$1 = 7 - 9(3) + 7(3)$

$1 = 7(4) + 9(-3)$

$7^{-1} \equiv 4 \bmod 9$

$y \equiv 4 \bmod 9$

$y = 9m + 4$

$x = 7(9m + 4) + 3$

$x = 63m + 28 + 3$

$x = 63m + 31$

$x \equiv 31 \bmod 63$

(b) $x \equiv 5 \bmod 9$

$x \equiv 6 \bmod 10$

$x \equiv 7 \bmod 11$

$5 + 9y = 6 \bmod 10$

$9y \equiv 1 \bmod 10$

$9^{-1} \equiv 1 \bmod 10 \rightarrow 9^{-1} \equiv 9 \bmod 10$

$x = 5 + 9(10m + 9) = x = 86 \bmod 90 \quad y = 9, \quad y = 10m + 9$

$x = 90y + 86, \quad 90 \equiv 2 \bmod 11$

$x = 2y + 86 \equiv 7 \bmod 11$

$x = 2y + 9 \equiv 7 \bmod 11$

$2y \equiv -2 \bmod 11$

Find $2^{-1} = 1 \bmod 11$

$2^{-1} \equiv 6 \bmod 11, \rightarrow 6 \cdot 9 \equiv 56 \equiv 10 \bmod 11$

$k = 11m + 10 \rightarrow$ Sub

$k = 11m + 10$

$x = 90(11m + 10) + 86 = 990m + 986$

$x \equiv 986 \bmod 990$

4

(a) $a = 9, m = 18$

$x^2 = 9 \bmod 18 \quad x = 0, \dots, 17$

x	$x^2 \bmod 18$
0	0
1	1
2	4
3	9
4	16
5	7
6	0
7	13
8	10
9	9
10	10
11	13
12	0
13	7
14	16
15	9
16	4
17	1

(a) $x = 3, 9, 15$

(b) $a = 28, m = 29$

$x^2 = 28 \bmod 29$

x	$x^2 \bmod 29$
0	0
1	1
2	4
3	9
4	16
5	25
6	7
7	20
8	6
9	23
10	13
11	5
12	28
13	24
14	22

x	$x^2 \bmod 29$
15	22
16	24
17	28
18	5
19	13
20	23
21	6
22	20
23	7
24	25
25	16
26	9
27	4
28	1

(b) $x = 12, 17$

5.

(a) $a = 3, m = 23$

(b) $a = 6, m = 43$

(a) $x^2 = 3 \bmod 23$

$3^{\frac{23-1}{3}} \equiv 3^{11} \bmod 23$

$3^1 \equiv 3 \bmod 23$

$3^2 \equiv 9 \bmod 23$

$3^4 = 81 \equiv 12 \bmod 23$

$3^8 = 144 \equiv 6 \bmod 23$

$3^{11} = 3 \times 9 \times 6 \equiv 1 \bmod 23$

$1^2 \bmod 23 = 1$ ✓

Find $x^2 \equiv 3 \bmod 23$

$23 \equiv 3 \bmod 4$

↳ $x \equiv 3^{\frac{23+1}{4}} \bmod 23$

$= x \equiv 3^6 \bmod 23$

↳ $3^6 = 729 \equiv 16 \bmod 23$

$3^6 \equiv 16 \bmod 23$

AND

$23 - 16 \equiv 7 \bmod 23$

(b) $6^{\frac{43-1}{6}} = 6^{11} \bmod 43$

$6^{21} \equiv 1 \bmod 43$ ✓

So, $43 = 6^{\frac{43+1}{4}} = 6^{11} \bmod 43$

Find $6^{11} \bmod 43$

$6^1 \equiv 6 \bmod 43$

$6^2 \equiv 36 \bmod 43$

$6^4 \equiv 6 \bmod 43$

$6^8 \equiv 36 \bmod 43$

$6^{11} \equiv 36 \times 36 \times 6 \equiv 7 \bmod 43$

$x = -7, 7$

$x = 7$

AND $-7 = 43 - 7 = 36 \bmod 43$

6. Theorem 7. $b \equiv a^{p+1/4} \bmod p$

$p = 211$, $a = 2$

$b = 2^{211+1/4} \bmod 211$

$b = 2^{53} \bmod 211$

$2^2 = 4 \bmod 211$

$2^4 = 16 \bmod 211$

$2^8 = 45 \bmod 211$

$2^{16} = 126 \bmod 211$

$2^{32} = 51 \bmod 211$

$2^{53} = 51 \times 126 \times 16 \times 2 \equiv 118 \bmod 211$

check $118^2 \bmod 211 \rightarrow 209 \neq 2$

NOT VALID Square Root