1.16. Write out the following tables for $\mathbb{Z}/m\mathbb{Z}$ and $(\mathbb{Z}/m\mathbb{Z})^*$, as we did in Figs. 1.4 and 1.5.

(d) Make a multiplication table for the unit group $(\mathbb{Z}/16\mathbb{Z})^*$.

For $(\mathbb{Z}/16\mathbb{Z})$

From homework 2: $(\mathbb{Z}/16\mathbb{Z})^* = \{1, 3, 5, 7, 9, 11, 13, 15\}$

•	1	3	5	7	9	11	13	15
1	1	3	5	7	9	11	13	15
3	3	9	15	5	11	1	7	13
5	5	15	9	3	13	7	1	11
7	7	5	3	1	15	13	11	9
9	9	11	13	15	1	3	5	7
11	11	1	7	13	3	9	15	5
13	13	7	1	11	5	15	9	3
15	15	13	11	9	7	5	3	1

$$\begin{array}{r} 25 \\ -16 \\ \hline 9 \end{array} \qquad \begin{array}{r} 49 \\ 32 \\ \hline 17 = 1 \end{array} \qquad \begin{array}{r} 7\ 81 \\ -64 \\ \hline 17 \end{array} \qquad \begin{array}{r} 7\,r\,9 \\ 16\overline{)121} \\ -112 \\ \hline 009 \end{array}$$

$$\begin{array}{r} 121 \\ -16 \\ \hline 05 \end{array}$$

1.26. Use the square-and-multiply algorithm described in Sect. 1.3.2, or the more efficient version in Exercise 1.25, to compute the following powers.
(a) $17^{183} \pmod{256}$.
(b) $2^{477} \pmod{1000}$.

Square-and-Multiply Algorithm. To compute $g^A \pmod N$:

(1) Compute the binary expansion of A as

$$A = A_0 + A_1 \cdot 2 + A_2 \cdot 2^2 + A_3 \cdot 2^3 + \cdots + A_r \cdot 2^r \quad \text{with } A_i \in \{0,1\} \text{ and } A_r = 1$$

(2) Compute $g^{2^i} \pmod N$ for $0 \le i \le r$ by successive squaring,

$$\begin{aligned} a_0 &\equiv g && \pmod N \\ a_1 &\equiv g^2 \equiv a_0^2 && \pmod N \\ a_2 &\equiv g^{2^2} \equiv a_1^2 && \pmod N \\ a_3 &\equiv g^{2^3} \equiv a_2^2 && \pmod N \\ &\vdots \\ a_r &\equiv g^{2^r} \equiv a_{r-1}^2 && \pmod N \end{aligned}$$

(3) Compute $g^A \pmod N$ using

$$\begin{aligned} g^A &= g^{A_0 + A_1 \cdot 2 + A_2 \cdot 2^2 + \cdots + A_r \cdot 2^r} \\ &= g^{A_0} \cdot (g^2)^{A_1} \cdot (g^{2^2})^{A_2} \cdots (g^{2^r})^{A_r} \\ &\equiv a_0^{A_0} \cdot a_1^{A_1} \cdot a_2^{A_2} \cdots a_r^{A_r} \pmod N \end{aligned}$$

(a)

$183 = 1 + 2 + 4 + 16 + 32 + 128$

To binary → $\underset{128}{1}\ \underset{64}{0}\ \underset{32}{1}\ \underset{16}{1}\ \underset{8}{0}\ \underset{4}{1}\ \underset{2}{1}\ \underset{1}{1}$

1 $\quad 17^1 \equiv 17 \pmod{256}$
1 $\quad 17^2 \equiv 33 \pmod{256}$
1 $\quad 17^4 = 83521/256 = 326r \equiv 65 \pmod{256}$
$\quad 256 \times 326 = 83456$
0 $\quad 17^8 = 65 \times 65 = 4225 \equiv 129 \pmod{256}$
1 $\quad 17^{16} = 129 \times 129 = 16641 \equiv 1 \pmod{256}$
1 $\quad 17^{32} = 1 \times 1 = 1 \pmod{256}$
0 $\quad 17^{64} = 1 \times 1 = 1 \pmod{256}$
1 $\quad 17^{128} = 1 \times 1 = 1 \pmod{256}$

CALCULATE:

$1 \times 1 \times 1 = 1 \bmod 256$

$1 \times 65 = 65 \bmod 256$

$65 \times 33 = 2145/256$
$= 8$ remainder

$$\begin{array}{r} 2145 \\ -2048 \\ \hline 97 \bmod 256 \end{array}$$

$$\begin{array}{r} 97 \times 17 = 1649 = 6 \\ -1536 \\ \hline 113 \bmod 256 \end{array}$$

ANSWER:

$17^{183} \equiv 113 \bmod 256$

1.26

(b) 2^{477} mod 1000

$477 = \frac{1}{256}\ \frac{1}{128}\ \frac{1}{64}\ \frac{0}{32}\ \frac{1}{16}\ \frac{1}{8}\ \frac{1}{4}\ \frac{0}{2}\ \frac{1}{1}$

$2^{477} = 2^{256} \cdot 2^{128} \cdot 2^{64} \cdot 2^{32} \cdot 2^{16} \cdot 2^{8} \cdot 2^{4} \cdot 2^{1}$

1 $2^1 \equiv 2$ mod 1000
1 $2^4 \equiv 16$ mod 1000
1 $2^8 \equiv 256$ mod 1000
1 $2^{16} = 65 \times 1000 \equiv 536$ mod 1000
0 $2^{36} = 287296 \equiv 296$ mod 1000
1 $2^{64} \equiv 616$ mod 1000
1 $2^{128} = 456$ mod 1000
1 $2^{256} = 936$ mod 1000

$\rightarrow 936 \times 456 \equiv 816$ mod 1000
$\rightarrow 816 \times 616 \equiv 656$ mod 1000
$\rightarrow 656 \times 536 \equiv 616$ mod 1000
$\rightarrow 616 \times 256 \equiv 696$ mod 1000
$\rightarrow 696 \times 16 \equiv 136$ mod 1000
$\rightarrow 136 \times 2 \equiv 272$ mod 1000

$2^{477} = 272$ mod 1000

1.30. Compute the following ord_p values:
(a) $\text{ord}_2(2816)$.
(b) $\text{ord}_7(2222574487)$.
(c) $\text{ord}_p(46375)$ for each of $p = 3, 5, 7$, and 11.

(c) $46375^k \equiv$ mod p

$\text{ord}_3(46375) : 0$
$\text{ord}_5(46375) : 3$
$\text{ord}_7(46375) : 1$
$\text{ord}_{11}(46375) : 0$

$46375 \div 5 = 9275$
$9275 \div 5 = 1855$
$1855 \div 5 = 371$ Not divisible by 5
For 7: $46375 = 4+6+3+7+5 = 25$ Not div by 3
$46375 = 5^3 \times 7^1 \times 53$

1.32. For each of the following primes p and numbers a, compute $a^{-1} \bmod p$ in two ways: (i) Use the extended Euclidean algorithm. (ii) Use the fast power algorithm and Fermat's little theorem. (See Example 1.27.)

(a) $p = 47$ and $a = 11$.
(b) $p = 587$ and $a = 345$.
(c) $p = 104801$ and $a = 78467$.

(a) $11^{-1} \bmod 47$

(i) $11u + 47v = 1$

$47 = 4 \times \underline{11} + 3$
$11 = \underline{3} \times 3 + 2$
$3 = 1 \times 2 + 1$
$2 = 2 \times 1 + 0 \leftarrow \gcd(11, 47) = 1$

$1 = 3 - 1 \times 2$
$1 = 3 - 1(11 - 3 \times 3) = 3 - 1 \times 11 + 3 \times 3$
$1 = (47 - 4 \times 11) - 1 \times 11 + 3(47 - 4 \times 11)$
$1 = 47 - 4 \times 11 - 11 + 3 \times 47 - 12 \times 11$
$1 = 4 \times 47 - 17 \times 11, \quad u = -17 \quad v = 4$

$11^{-1} \equiv 30 \bmod 47$

$47 - 17 = 30$

(ii) $11^{p-1-1} = 11^{45} \equiv 1 \bmod 47$

Square AND MULTIPLY

$45 = \underset{32}{1}\ \underset{16}{0}\ \underset{8}{1}\ \underset{4}{1}\ \underset{2}{0}\ \underset{1}{1}$

0 $11^2 = 121 \equiv 27 \bmod 47$
1 $11^4 = 27^2 = 729 \equiv 25 \bmod 47$
1 $11^8 = 25^2 = 625 \equiv 14 \bmod 47$
0 $11^{16} = 14^2 = 196 \equiv 8 \bmod 47$
1 $11^{32} = 8^2 = 64 \equiv 17 \bmod 47$

multiply:

$11^{45} = 11^{32} \times 11^8 \times 11^4 \times 11$
$11^{45} = 17 \times 14 \times 25 \times 11$
$11^{45} \equiv 30 \bmod 47$

$11^{-1} \equiv 30 \bmod 47$

(b) (i) $345u + 587v = 1$

$587 = 1 \times 345 + 242$
$345 = 1 \times 242 + 103$
$242 = 2 \times 103 + 36$
$103 = 2 \times 36 + 31$
$36 = 1 \times 31 + 5$
$31 = 6 \times 5 + 1$
$5 = 5 \times 1 + 0$
$\gcd(345, 587) = 1$

$\begin{array}{r} 67 \\ +47 \\ \hline 114 \end{array}$ $\quad u = 114$

Sub back in:

$1 = 31 - 6 \times 5$
$1 = 31 - 6(36 - 1 \times 31) = 7 \times 31 - 6 \times 36$
$1 = 7(103 - 2 \times 36) - 6 \times 36$
$1 = 7 \cdot 103 - 20 \times 36$
$1 = 7 \cdot 103 - 20(242 - 2 \cdot 103)$
$1 = -20 \times 242 + 47 \cdot 103$
$1 = 47 \times 345 - 1 \times 242 - 20 \times 242$
$1 = 47 \times 345 - 67 \times 242$
$1 = 47 \times 345 - 67(587 - 1 \times 345)$
$1 = 114 \times 345 - 67 \times 587$

$345^{-1} \equiv 114 \bmod 587$

(ii) $345^{-1} = 345^{585} \bmod 587$

$587 = \frac{1}{512}\ \frac{0}{256}\ \frac{0}{128}\ \frac{1}{64}\ \frac{0}{32}\ \frac{0}{16}\ \frac{1}{8}\ \frac{0}{4}\ \frac{1}{2}\ \frac{1}{1}$

1 $345^2 \equiv 381 \bmod 587$

$345^4 = 381^2 \equiv 128 \bmod 587$

1 $345^8 = 128^2 \equiv 557 \bmod 587$

$345^{16} = 557^2 \equiv 196 \bmod 587$

$345^{32} = 196^2 \equiv 515 \bmod 587$

1 $345^{64} = 515^2 \equiv 319 \bmod 587$

$345^{128} = 319^2 \equiv 502 \bmod 587$

$345^{256} = 502^2 \equiv 216 \bmod 587$

1 $345^{512} = 216^2 \equiv 283 \bmod 587$

$345 \times 557 \times 319 \times 283 \equiv 114$

$345^{-1} \equiv 114 \bmod 587$

1.34. Recall that g is called a primitive root modulo p if the powers of g give all nonzero elements of $\mathbb{F}_p$.

(a) For which of the following primes is 2 a primitive root modulo p?

(i) $p = 7$ (ii) $p = 13$ (iii) $p = 19$ (iv) $p = 23$

$2^k \equiv 1 \bmod p$

$k = p - 1$

(a)

(i) $2^1 \equiv 2 \bmod 7$

$2^2 \equiv 4 \bmod 7$

$2^3 \equiv 1 \bmod 7$

No

(ii) $2^1 \equiv 2 \bmod 13$

$2^2 \equiv 4 \bmod 13$

$2^3 = 8 \bmod 13$

$2^4 \equiv 3 \bmod 13$

$2^5 \equiv 6 \bmod 13$

$2^6 \equiv 12 \bmod 13$

$2^7 \equiv 11 \bmod 13$

$2^8 \equiv 9 \bmod 13$

$2^9 \equiv 5 \bmod 13$

$2^{10} \equiv 10 \bmod 13$

$2^{11} \equiv 7 \bmod 13$

$2^{12} \equiv 1 \bmod 13$

YES

(iii) $2^{13} = 3 \ m19$

$2^{14} = 6 \ m19$

$\vdots$

$2^{16} = 5 \ m19$

$2^{18} = 1 \bmod 19$

YES

(iv) $2^{11} \equiv 22 \equiv -1 \bmod 23$

$2^{22} \equiv 1 \bmod 23$

No

(b) For which of the following primes is 3 a primitive root modulo p?

(i) $p = 5$ (ii) $p = 7$ (iii) $p = 11$ (iv) $p = 17$

(c) Find a primitive root for each of the following primes.

(i) $p = 23$ (ii) $p = 29$ (iii) $p = 41$ (iv) $p = 43$

$2^k \equiv 1 \bmod p$

$k = p-1$

(b)

(i) $p=5$

$3^1 \equiv 3 \bmod 5$

$3^2 \equiv 4 \bmod 5$

$3^3 \equiv 2 \bmod 5$

$3^4 \equiv 1 \bmod 5$

YES

(ii) $3^6 \equiv 1 \bmod 7$

$6 = p-1 \to 6 = 7-1$ ✓

YES

(iii)

$3^4 \equiv 4 \bmod 11$

$3^5 \equiv 1 \bmod 11$

$11-1 \neq 5$

NO

(iv) :

$3^{16} \equiv 1 \bmod 17$

$17-1 = 16$ ✓

YES

(c) $g^k \equiv 1 \bmod p$ smallest $k = p-1$

(i) $p = 23$

$5^{11} \equiv -1 \bmod 23$

$5^{11} = (5^5)^2 \times 5 \bmod 23$

⋮

$5^{10} = 20^2 = 400 \equiv 9 \bmod 23$

$5^{11} = 9 \times 5 = 45 \equiv 22 \equiv -1 \bmod 23$

$g = 5$

(ii) $p = 29$

$2^{28} \equiv 1 \bmod 29$

$2^2 = 4$

$2^4 = 16$

$2^7 = 16 \times 2^3 = 16 \times 8 = 128 \equiv 12 \bmod 29$

$2^{14} = 12^2 = 144 \equiv 28 \equiv -1 \bmod 29$ ✓

$g = 2$

(iv) $p-1 = 42 = 2 \times 3 \times 7$

$3^2 = 9$

$3^3 = 27$, $3^7 \equiv 40 \bmod 43$

$3^{14} \equiv 4 \bmod 43$

$3^{21} \equiv 31 \bmod 43$

$g = 3$

(iii) $p-1 = 40 = 2^3 \times 5$

$6^{20} \equiv X \bmod 41$

$6^2 = 36 \equiv -5 \bmod 41$

$6^4 = (-5)^2 = 25 \bmod 41$

$6^5 = 25 \times 6 = 150 \equiv 26 \bmod 41$

$6^{10} = 26^2 = 676 \equiv 20 \bmod 41$

$6^{20} = 20^2 = 400 \equiv 29 \bmod 41$

$g = 6$