

**Problem 1.** (10 points) Here is a table of powers of 23 modulo 167.

$$\begin{array}{ll} 23^1 \equiv 23 \pmod{167} & 23^{32} \equiv 126 \pmod{167} \\ 23^2 \equiv 28 \pmod{167} & 23^{64} \equiv 11 \pmod{167} \\ 23^4 \equiv 116 \pmod{167} & 23^{128} \equiv 121 \pmod{167} \\ 23^8 \equiv 96 \pmod{167} & 23^{256} \equiv 112 \pmod{167} \\ 23^{16} \equiv 31 \pmod{167} & \end{array}$$

Use the table to compute  $23^{78} \pmod{167}$ . Your answer should be an integer between 0 and 166.

**Solution.** First we compute the binary expansion of the exponent:

$$78 = 64 + 8 + 4 + 2.$$

Then

$$23^{78} = 23^{64} \cdot 23^8 \cdot 23^4 \cdot 23^2 \equiv 11 \cdot 96 \cdot 116 \cdot 28 \equiv 3429888 \equiv 42 \pmod{167}.$$

**Problem 2.** (10 points) Find a solution to the pair of simultaneous congruences

$$x \equiv 15 \pmod{117} \quad \text{and} \quad x \equiv 37 \pmod{118}.$$

**Solution.** The solutions to the first congruence look like  $x = 15 + 117y$ . Substituting into the second congruence, we get

$$15 + 117y \equiv 37 \pmod{118}.$$

Since  $117 \equiv -1 \pmod{118}$ , this is  $-y \equiv 22 \pmod{118}$ , so  $y \equiv -22 \equiv 96 \pmod{118}$ . Hence the solution to the original problem is

$$x = 15 + 117y = 15 + 117 \cdot 96 = 11247.$$

**Problem 3.** (10 points) Let  $p$  be a prime such that  $p > 10$ . Find an integer  $N$  between 1 and 1000 that satisfies

$$N \equiv 5^{4p} \pmod{12p}.$$

**Solution.** Euler's formula tells us that  $a^{\phi(12p)} \equiv 1 \pmod{12p}$ . The Euler phi function is multiplicative, so  $\phi(12p) = \phi(4)\phi(3)\phi(p) = 2 \cdot 2 \cdot (p-1) = 4(p-1)$ , so  $a^{4(p-1)} \equiv 1 \pmod{12p}$ . Multiplying by  $a^4$ , we see that

$$a^{4p} \equiv a^4 \pmod{12p}.$$

Taking  $a = 5$  gives

$$5^{4p} \equiv 5^4 \equiv 625 \pmod{12p}.$$

**Problem 4.** (24 points) NOTE: For this problem only, you need not show your work, since only your answer will be counted.

**Grading:** +4 for each correct answer, −2 for each incorrect answer.

Your answers must go in the box at the bottom of the page. No credit will be given for answers that appear elsewhere.

- (a) What is the value of  $\left(\frac{42}{229}\right)$ ?
- (b) Does the congruence  $x^2 \equiv 23 \pmod{131}$  have a solution?
- (c) What is the value of  $\left(\frac{-45}{331}\right)$ ?
- (d) Does the congruence  $x^2 + 4x - 7 \equiv 0 \pmod{89}$  have a solution?
- (e) If  $\left(\frac{a}{p}\right) = 1$ ,  $\left(\frac{b}{p}\right) = -1$ , and  $\left(\frac{c}{p}\right) = -1$ , what is the value of  $\left(\frac{abc^2}{p}\right)$ ?
- (f) If  $p \equiv 3 \pmod{8}$ , what is the value of  $\left(\frac{-2}{p}\right)$ ?

**Solution.** (a)  $\left(\frac{42}{229}\right) = \left(\frac{2}{229}\right)\left(\frac{21}{229}\right) = -\left(\frac{21}{229}\right) = -\left(\frac{229}{21}\right) = -\left(\frac{19}{21}\right) = -\left(\frac{21}{19}\right) = -\left(\frac{2}{19}\right) = 1$ .

(b)  $\left(\frac{23}{131}\right) = -\left(\frac{131}{23}\right) = -\left(\frac{16}{23}\right) = -1$ , so no solution.

(c)  $\left(\frac{-45}{331}\right) = \left(\frac{-1}{331}\right)\left(\frac{45}{331}\right) = -\left(\frac{45}{331}\right) = -\left(\frac{331}{45}\right) = -\left(\frac{16}{45}\right) = -1$ .

(d) The quadratic formula says that the solution is  $(-4 \pm \sqrt{44})/2$ , so there will be a solution if and only if 44 is a square modulo 89. We compute  $\left(\frac{44}{89}\right) = \left(\frac{2^2}{89}\right)\left(\frac{11}{89}\right) = \left(\frac{11}{89}\right) = \left(\frac{89}{11}\right) = \left(\frac{1}{11}\right) = 1$ . So there is a solution. (It turns out that the solutions are 8 and 77.)

(e) By multiplicativity of the Legendre symbol,  $\left(\frac{abc^2}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)\left(\frac{c}{p}\right)^2 = 1 \cdot (-1) \cdot (-1)^2 = -1$ .

(f) Note that  $p \equiv 3 \pmod{8}$  implies that  $p \equiv 3 \pmod{4}$ , so  $\left(\frac{-1}{p}\right) = -1$  and  $\left(\frac{2}{p}\right) = -1$ . Hence  $\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right) = (-1)(-1) = 1$ .

To summarize:

(a) 1      (b) NO      (c) −1      (d) YES      (e) −1      (f) 1

**Problem 5.** (10 points) The integer  $m$  has the property that

$$37 \cdot 193 \equiv 1 \pmod{m} \quad \text{and} \quad 37 \cdot 214 \equiv 1 \pmod{\phi(m)}.$$

Further, the powers of  $a$  modulo  $m$  are given in the following table:

$$\begin{array}{ll} a \equiv a \pmod{m} & a^{32} \equiv f \pmod{m} \\ a^2 \equiv b \pmod{m} & a^{64} \equiv g \pmod{m} \\ a^4 \equiv c \pmod{m} & a^{128} \equiv h \pmod{m} \\ a^8 \equiv d \pmod{m} & a^{256} \equiv i \pmod{m} \\ a^{16} \equiv e \pmod{m} & \end{array}$$

Find the solution to

$$x^{37} \equiv a \pmod{m}.$$

Your answer should be expressed using the numbers  $a, b, c, \dots, i$ , but no number in the list  $a, b, c, \dots, i$  should appear more than once in your answer.

**Solution.** We are told that  $37 \cdot 214 = 1 + u\phi(m)$  for some  $u$ , so raising to the 214 power, we have

$$x^{37 \cdot 214} = x^{1+u\phi(m)} \equiv x \pmod{m}.$$

(Here we use Euler's formula, which says that  $A^{\phi(m)} \equiv 1 \pmod{m}$ .) Thus

$$x \equiv x^{37 \cdot 214} \equiv a^{214} \pmod{m}.$$

Next we compute the binary expansion of 214,

$$214 = 128 + 64 + 16 + 4 + 2,$$

so

$$a^{214} = a^{128+64+16+4+2} = a^{128} a^{64} a^{16} a^4 a^2 \equiv hgecb \pmod{m}.$$