Math 393
10-11-2020

Review Problems for Test 3

These problems are provided to help you study. The presence of a problem on this handout does not imply that there *will* be a similar problem on the test. And the absence of a topic does not imply that it *won't* appear on the test.

1. Find the decoding transformation for the affine transformation cipher

$$C = 15P + 7 \pmod{26}.$$

2. Find the decoding transformation for the digraphic cipher

$$\begin{bmatrix} C_1 \\ C_2 \end{bmatrix} = \begin{bmatrix} 7 & 5 \\ 5 & 10 \end{bmatrix} \begin{bmatrix} P_1 \\ P_2 \end{bmatrix} \pmod{26}.$$

3. Calvin Butterball constructs the following digraphic cipher:

$$\begin{bmatrix} C_1 \\ C_2 \end{bmatrix} = \begin{bmatrix} 7 & 4 \\ 2 & 3 \end{bmatrix} \begin{bmatrix} P_1 \\ P_2 \end{bmatrix} \pmod{26}.$$

Show that this is a bad idea by finding two different plaintext blocks that give the same ciphertext block.

4. Find the decoding transformation for the exponential cipher

$$C = P^{23} \pmod{5003}.$$

5. Suppose that $n = 80609$ is a product of two primes p and q, and that $\phi(n) = 79920$. Without factoring n directly, find p and q.

6. (a) Use an RSA cipher with $n = 4141 = 41 \cdot 101$ and exponent 27 to encipher the word OMELET.

(b) Find the decoding transformation for the cipher in part (a).

7. Find a solution to the following quadratic congruence.

$$x^2 = 280 \pmod{529}.$$

(Note that $529 = 23^2$.)

8. Solve $x^2 = 33 \pmod{527}$. [Note: $527 = 17 \cdot 31$.]

9. Find the quadratic residues mod 17.

10. Find the quadratic residues mod 18.

11. Compute the following Legendre symbols:

(a) $\left(\dfrac{71}{79}\right)$.

(b) $\left(\dfrac{72}{79}\right)$.

(c) $\left(\frac{564}{569}\right)$.

(d) $\left(\frac{5}{55k+1}\right)$, if $55k+1$ is prime.

(e) Compute $\left(\frac{8}{31}\right)$.

12. Determine whether $x^2 = 1220 \pmod{1301}$ has solutions. (Note: 1301 is prime.)

13. State the Law of Quadratic Reciprocity in terms of congruences, and in terms of Legendre symbols.

14. Show that if p is an odd prime and 2, 3, and 6 are distinct mod p, then at least one of 2, 3, or 6 is a quadratic residue mod p.

15. Use Gauss's lemma to determine whether $x^2 = 15 \pmod{17}$ has any solutions.

16. Compute the following Jacobi symbols.

(a) $\left(\frac{37}{297}\right)$.

(b) $\left(\frac{175}{213}\right)$.

17. Let p be an odd prime. Prove that

$$\left(\frac{-2}{p}\right) = \begin{cases} 1 & \text{if } p = 8k+1 \text{ or } p = 8k+3 \\ -1 & \text{if } p = 8k+5 \text{ or } p = 8k+7 \end{cases}.$$

18. Convert $(7213)_8$ to base 10.

19. Convert 1808 to base 7.

20. Express 0.3 in base-7.

21. Express $(0.54242\ldots)_6 = (0.5\overline{42})_6$ as a decimal fraction in lowest terms.

22. Let b be a positive integer greater than 3. Express $(0.3(b-1)3(b-1)\ldots)_b = (0.\overline{3(b-1)})_b$ as a rational function of b.

23. Let b be a positive integer greater than 3. Find the base b expansion of $\dfrac{2b^2+1}{b^2-1}$.

24. Find the finite continued fraction expansion for $\dfrac{983}{237}$.

25. Find the successive convergents and the exact value of the finite continued fraction $[3, 1, 4, 1, 1, 6]$.

26. Suppose x is a positive integer. Find the exact value of

$$1 + \cfrac{1}{x + \cfrac{1}{x^2 + \cfrac{1}{x^3}}}.$$

27. Use continued fractions to find an integer linear combination of 501 and 113 which is equal to 1.

Solutions to the Review Problems for Test 3

1. Find the decoding transformation for the affine transformation cipher

$$C = 15P + 7 \pmod{26}.$$

26	-	7
15	1	4
11	1	3
4	2	1
3	1	1
1	3	0

$$1 = (-4)(26) + (7)(15), \quad \text{so} \quad 7 = 15^{-1} \pmod{26}.$$

Therefore,

$$\begin{aligned} C &= 15P + 7 \pmod{26} \\ C - 7 &= 15P \pmod{26} \\ C + 19 &= 15P \pmod{26} \\ 7(C + 19) &= P \pmod{26} \\ 7C + 3 &= P \pmod{26} \end{aligned}$$

---

2. Find the decoding transformation for the digraphic cipher

$$\begin{bmatrix} C_1 \\ C_2 \end{bmatrix} = \begin{bmatrix} 7 & 5 \\ 5 & 10 \end{bmatrix} \begin{bmatrix} P_1 \\ P_2 \end{bmatrix} \pmod{26}.$$

Find the inverse of the matrix:

$$\begin{bmatrix} 7 & 5 \\ 5 & 10 \end{bmatrix}^{-1} = (7 \cdot 10 - 5 \cdot 5)^{-1} \begin{bmatrix} 10 & -5 \\ -5 & 7 \end{bmatrix} = 45^{-1} \cdot \begin{bmatrix} 10 & -5 \\ -5 & 7 \end{bmatrix} \pmod{26}.$$

Use the Euclidean algorithm to compute $45^{-1} \pmod{26}$:

45	-	19
26	1	11
19	1	8
7	2	3
5	1	2
2	2	1
1	2	0

Thus,

$$(11)(45) + (-19)(26) = 1, \quad \text{so} \quad (11)(45) = 1 \pmod{26}.$$

Therefore, $45^{-1} = 11 \pmod{26}$, and the inverse matrix is

$$11 \cdot \begin{bmatrix} 10 & -5 \\ -5 & 7 \end{bmatrix} = \begin{bmatrix} 110 & -55 \\ -55 & 77 \end{bmatrix} = \begin{bmatrix} 6 & 23 \\ 23 & 25 \end{bmatrix} \pmod{26}.$$

The decoding transformation is

$$\begin{bmatrix} P_1 \\ P_2 \end{bmatrix} = \begin{bmatrix} 6 & 23 \\ 23 & 25 \end{bmatrix} \begin{bmatrix} C_1 \\ C_2 \end{bmatrix} \pmod{26}. \quad \square$$

---

3. Calvin Butterball constructs the following digraphic cipher:

$$\begin{bmatrix} C_1 \\ C_2 \end{bmatrix} = \begin{bmatrix} 7 & 4 \\ 2 & 3 \end{bmatrix} \begin{bmatrix} P_1 \\ P_2 \end{bmatrix} \pmod{26}.$$

Show that this is a bad idea by finding two different plaintext blocks that give the same ciphertext block.

The problem, of course, is that

$$\begin{vmatrix} 7 & 4 \\ 2 & 3 \end{vmatrix} = 13 \quad \text{and} \quad (13, 26) = 13 \neq 1.$$

I want P_1, P_2, P_1', P_2', such that $(P_1, P_2) \neq (P_1', P_2')$, but

$$\begin{bmatrix} 7 & 4 \\ 2 & 3 \end{bmatrix} \begin{bmatrix} P_1 \\ P_2 \end{bmatrix} = \begin{bmatrix} 7 & 4 \\ 2 & 3 \end{bmatrix} \begin{bmatrix} P_1' \\ P_2' \end{bmatrix} \pmod{26}.$$

Moving all the terms to the left side and factoring, I have

$$\begin{bmatrix} 7 & 4 \\ 2 & 3 \end{bmatrix} \begin{bmatrix} P_1 - P_1' \\ P_2 - P_2' \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix} \pmod{26}.$$

I see that what I need is a nontrivial (i.e. nonzero) solution to the homogeneous system

$$\begin{bmatrix} 7 & 4 \\ 2 & 3 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix} \pmod{26}.$$

To do this, row reduce. To find out how to "divide" the first row by 7, use the Extended Euclidean Algorithm:

26	-	11
7	3	3
5	1	2
2	2	1
1	2	0

$$1 = (26, 7) = 26 \cdot 3 + 7 \cdot (-11)$$
$$1 = 7 \cdot (-11) \pmod{26}$$
$$1 = 7 \cdot 15 \pmod{25}$$

Thus,

$$\begin{bmatrix} 7 & 4 \\ 2 & 3 \end{bmatrix} \underset{r_1 \to 15 r_1}{\to} \begin{bmatrix} 1 & 8 \\ 2 & 3 \end{bmatrix} \underset{r_2 \to r_2 + 24 r_1}{\to} \begin{bmatrix} 1 & 8 \\ 0 & 13 \end{bmatrix} \pmod{26}.$$

I can't go any further, because 13 isn't invertible mod 26.

These equations say

$$\begin{aligned} x + 8y &= 0 \pmod{26} \\ 13y &= 0 \pmod{26} \end{aligned}$$

I want a nonzero solution. So take $y = 2$ to satisfy the second equation. (Any even number will work for y.) Plugging this into the first equation, I get

$$x + 16 = 0, \quad \text{or} \quad x = 10.$$

Finally, recall that (x, y) represents $(P_1 - P_1', P_2 - P_2')$. So to get two different plaintexts that give the same ciphertext, set (P_1', P_2') to anything — say $(0, 0)$ — and add $(10, 2)$ to get $(P_1, P_2) = (10, 2)$.

You can check that

$$\begin{bmatrix} 7 & 4 \\ 2 & 3 \end{bmatrix} \begin{bmatrix} P_1 \\ P_2 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix} \pmod{26} \quad \text{and} \quad \begin{bmatrix} 7 & 4 \\ 2 & 3 \end{bmatrix} \begin{bmatrix} P_1' \\ P_2' \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix} \pmod{26}.$$

Try setting $(P_1', P_2') = (1, 5)$ (say), so $(P_1, P_2) = (10 + 1, 5 + 2) = (11, 7)$. You can verify for yourself that this choice of (P_1, P_2) and (P_1', P_2') will work as well. $\square$

---

4. Find the decoding transformation for the exponential cipher

$$C = P^{23} \pmod{5003}.$$

I need to find $23^{-1} \pmod{5002}$.

5002	-	435
23	217	2
11	2	1
1	11	0

$$\begin{aligned} 435 \cdot 23 - 2 \cdot 5002 &= 1 \\ 435 \cdot 23 &= 1 \pmod{5002} \end{aligned}$$

$23^{-1} = 435 \pmod{5002}$, so the decoding transformation is

$$P = C^{435} \pmod{5003}. \quad \square$$

Note: The inverse must be converted to a positive number before being used as the exponent in the decoding transformation. For example, if the original exponent had been 19, then

$$19^{-1} = -1053 = 3949 \pmod{5002}.$$

The decoding transformation would then be $P = C^{3949} \pmod{5003}$.

---

5. Suppose that $n = 80609$ is a product of two primes p and q, and that $\phi(n) = 79920$. Without factoring n directly, find p and q.

I have

$$\phi(n) = \phi(pq) = (p - 1)(q - 1) = n - (p + q) + 1, \quad \text{so} \quad p + q = n - \phi(n) + 1.$$

Thus,

$$p + q = 80609 - 79920 + 1 = 690.$$

In addition,

$$p - q = \sqrt{(p+q)^2 - 4pq} = \sqrt{(p+q)^2 - 4n}.$$

Therefore,

$$p - q = \sqrt{690^2 - 4 \cdot 80609} = 392.$$

So

$$2p = (p+q) + (p-q) = 1082, \quad \text{and} \quad p = 541.$$

Hence, $q = 690 - 541 = 149$. The primes are 149 and 541. $\square$

---

6. (a) Use an RSA cipher with $n = 4141 = 41 \cdot 101$ and exponent 27 to encipher the word OMELET.

(b) Find the decoding transformation for the cipher in part (a).

(a) Note that $\phi(4141) = 40 \cdot 100 = 4000$, and $(27, 4000) = 1$.
since $2525 < 4141 < 252525$, I use blocks of 2 letters.
Translate OMELET to 1412 0411 0419. To encipher the first block, for example, I compute

$$1412^{27} = 1677 \pmod{4141}.$$

Proceeding in the same way, I obtain the ciphertext 1677 0288 1139. $\square$

(b) I need to find d such that $d \cdot 27 = 1 \pmod{4000}$. Use the Euclidean algorithm:

4000	-	1037
27	148	7
4	6	1
3	1	1
1	3	0

This means that

$$(7)(4000) + (-1037)(27) = 1, \quad \text{or} \quad (-1037)(27) = 1 \pmod{4000}.$$

Since $-1037 = 2963 \pmod{4000}$, I can take $d = 2963$. The decoding transformation is

$$P = C^{2963} \pmod{4141}. \quad \square$$

---

7. Find a solution to the following quadratic congruence.

$$x^2 = 280 \pmod{529}.$$

(Note that $529 = 23^2$.)

First, consider the congruence mod 23:

$$x^2 = 280 = 4 \pmod{23}.$$

Clearly, $x = 2$ is a solution.
I'll try to find a solution $y = 2 + 23z$ to the original congruence:

$$\begin{aligned} y^2 &= 280 \pmod{529} \\ (2+23z)^2 &= 280 \pmod{529} \\ 4 + 92z + 529z^2 &= 280 \pmod{529} \\ 92z &= 276 \pmod{529} \end{aligned}$$

Note that $276 = 3 \cdot 92$. Dividing the congruence by 92, I must divide the modulus by $(529, 92) = 23$:

$$z = 3 \pmod{23}.$$

Then a solution is given by

$$y = 2 + 23 \cdot 3 = 71 \pmod{529}.$$

Note that $y = -71 = 458 \pmod{529}$ also works. □

---

8. Solve $x^2 = 33 \pmod{527}$.

$527 = 17 \cdot 31$, so this is equivalent to solving

$$x^2 = 33 \pmod{17} \quad \text{and} \quad x^2 = 33 \pmod{31}.$$

$x^2 = 33 \pmod{17}$ becomes $x^2 = 16 \pmod{17}$, which has solutions $x = \pm 4 \pmod{17}$.
$x^2 = 33 \pmod{31}$ becomes $x^2 = 2 \pmod{31}$.

x	1	2	3	4	5	6	7	8
$x^2 \pmod{31}$	1	4	9	16	25	5	18	2
x	9	10	11	12	13	14	15	
$x^2 \pmod{31}$	19	7	28	20	14	10	8	

(I obviously don't need to check $x = 0$, and the squares from 16 to 30 repeat those from 1 to 15, backwards.)
The solutions are $x = \pm 8 \pmod{31}$.
Now take cases. If $x = 4 \pmod{17}$ and $x = 8 \pmod{31}$, then

$$\begin{aligned} x &= 4 + 17a \\ 4 + 17a &= 8 \pmod{31} \\ 17a &= 4 \pmod{31} \end{aligned}$$

I need to find $17^{-1} \pmod{31}$. Use the Extended Euclidean Algorithm:

31	-	11
17	1	6
14	1	5
3	4	1
2	1	1
1	2	0

$$1 = 11 \cdot 17 - 6 \cdot 31, \quad 1 = 11 \cdot 17 \pmod{31}.$$

Thus, $17^{-1} = 11 \pmod{31}$. So

$$\begin{aligned} 11 \cdot 17a &= 11 \cdot 4 \pmod{31} \\ a &= 44 = 13 \pmod{31} \\ a &= 13 + 31b \\ x &= 4 + 17(13 + 31b) \\ x &= 225 \pmod{527} \end{aligned}$$

If $x = 4 \pmod{17}$ and $x = -8 = 23 \pmod{31}$, then

$$\begin{aligned} x &= 4 + 17a \\ 4 + 17a &= 23 \pmod{31} \\ 17a &= 19 \pmod{31} \\ 11 \cdot 17a &= 11 \cdot 19 \pmod{31} \\ a &= 209 = 23 \pmod{31} \\ a &= 23 + 31b \\ x &= 4 + 17(23 + 31b) \\ x &= 395 \pmod{527} \end{aligned}$$

The other solutions are $x = -225 = 302 \pmod{527}$ and $x = -395 = 132 \pmod{527}$. All together, the solutions are $x = 132, 225, 302, 395 \pmod{527}$. $\square$

---

9. Find the quadratic residues mod 17.

x	1	2	3	4	5	6	7	8
$x^2 \pmod{17}$	1	4	9	16	8	2	15	13
x	9	10	11	12	13	14	15	16
$x^2 \pmod{17}$	13	15	2	8	16	9	4	1

The quadratic residues mod 17 are 1, 2, 4, 8, 9, 13, 15, and 16. $\square$

---

10. Find the quadratic residues mod 18.

x	0	1	2	3	4	5	6	7	8
$x^2 \pmod{18}$	0	1	4	9	16	7	0	13	10

x	9	10	11	12	13	14	15	16	17
$x^2 \pmod{18}$	9	10	13	0	7	16	9	4	1

Of the squares mod 18, only 1, 7, and 13 are relatively prime to 18. So the quadratic residues mod 18 are 1, 7, and 13. $\square$

---

11. Compute the following Legendre symbols:

(a) $\left(\frac{71}{79}\right)$.

(b) $\left(\frac{72}{79}\right)$.

(c) $\left(\frac{564}{569}\right)$.

(d) $\left(\frac{5}{55k+1}\right)$, if $55k+1$ is prime.

(e) $\left(\frac{8}{31}\right)$.

(a) Since $71 = 4 \cdot 17 + 3$ and $79 = 4 \cdot 19 + 3$, reciprocity gives

$$\left(\frac{71}{79}\right) = -\left(\frac{79}{71}\right) = -\left(\frac{8}{71}\right) = -\left(\frac{2}{71}\right) \cdot \left(\frac{4}{71}\right) = -\left(\frac{2}{71}\right) \cdot 1 = -\left(\frac{2}{71}\right).$$

Now if p is an odd prime,

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}.$$

So

$$\left(\frac{2}{71}\right) = (-1)^{(71^2-1)/8} = (-1)^{630} = 1.$$

Hence, $\left(\frac{71}{79}\right) = -1.$ $\square$

(b)

$$\left(\frac{72}{79}\right) = \left(\frac{36}{79}\right) \cdot \left(\frac{2}{79}\right) = 1 \cdot \left(\frac{2}{79}\right) = \left(\frac{2}{79}\right).$$

As in (a),

$$\left(\frac{2}{79}\right) = (-1)^{(79^2-1)/8} = (-1)^{780} = 1.$$

Thus, $\left(\frac{72}{79}\right) = 1.$ $\square$

(c) 569 is prime.
$564 = 3 \cdot 4 \cdot 47$, so

$$\left(\frac{564}{569}\right) = \left(\frac{3}{569}\right)\left(\frac{4}{569}\right)\left(\frac{47}{569}\right).$$

$\left(\frac{4}{569}\right) = 1$, because 4 is a perfect square.
$569 = 4 \cdot 142 + 1$, so

$$\left(\frac{3}{569}\right) = \left(\frac{569}{3}\right) = \left(\frac{2}{3}\right) = -1,$$

$$\left(\frac{47}{569}\right) = \left(\frac{569}{47}\right) = \left(\frac{5}{47}\right) = \left(\frac{47}{5}\right) = \left(\frac{2}{5}\right) = -1.$$

Therefore,

$$\left(\frac{564}{569}\right) = (-1)(1)(-1) = 1. \quad \square$$

(d) Since $5 = 4 \cdot 1 + 1$, Quadratic Reciprocity gives

$$\left(\frac{5}{55k+1}\right) = \left(\frac{55k+1}{5}\right) = \left(\frac{1}{5}\right) = 1. \quad \square$$

(e)

$$\left(\frac{8}{31}\right) = \left(\frac{4}{31}\right)\left(\frac{2}{31}\right) = 1 \cdot \left(\frac{2}{31}\right) = (-1)^{(31^2-1)/8} = (-1)^{120} = 1.$$

To compute $\left(\frac{2}{31}\right)$, I used the formula $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$. You could also compute the last symbol using Euler's Theorem. $\square$

---

12. Determine whether $x^2 = 1220 \pmod{1301}$ has solutions. (Note: 1301 is prime.)

$$\left(\frac{1220}{1301}\right) = \left(\frac{4}{1301}\right)\left(\frac{5}{1301}\right)\left(\frac{61}{1301}\right) = \left(\frac{5}{1301}\right)\left(\frac{61}{1301}\right) = \left(\frac{1301}{5}\right)\left(\frac{1301}{61}\right) = \left(\frac{1}{5}\right)\left(\frac{20}{61}\right) =$$

$$\left(\frac{4}{61}\right)\left(\frac{5}{61}\right) = \left(\frac{5}{61}\right) = \left(\frac{61}{5}\right) = \left(\frac{1}{5}\right) = 1.$$

Hence, $x^2 = 1220 \pmod{1301}$ has solutions. $\square$

---

13. State the Law of Quadratic Reciprocity in terms of congruences, and in terms of Legendre symbols.

Let p and q be distinct odd primes.
In terms of congruences, reciprocity says: Consider the congruences

$$x^2 = p \pmod{q} \quad \text{and} \quad x^2 = q \pmod{p}.$$

If either p or q has the form $4k+1$ for $k \in \mathbb{N}$, then both congruences have solutions or both do not have solutions.
If both $p = 4j+3$ and $q = 4k+3$ for $j, k \in \mathbb{N}$, then one congruence is solvable and the other is not.
In terms of Legendre symbols, reciprocity says:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{[(p^2-1)/2][(q^2-1)/2]}.$$

An equivalent statement in terms of symbols is this: If either p or q has the form $4k+1$ for $k \in \mathbb{N}$, then $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$.
If both $p = 4j+3$ and $q = 4k+3$ for $j, k \in \mathbb{N}$, then $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$. $\square$

---

14. Show that if p is an odd prime and 2, 3, and 6 are distinct mod p, then at least one of 2, 3, or 6 is a quadratic residue mod p.

I have

$$\left(\frac{6}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{3}{p}\right).$$

Suppose 2, 3, and 6 are quadratic nonresidues mod p. Then all three of the symbols $\left(\frac{6}{p}\right)$, $\left(\frac{2}{p}\right)$, and $\left(\frac{3}{p}\right)$ are -1, and the equation above says "$-1 = (-1)(-1)$", a contradiction. Hence, at least one of the three is a quadratic residue mod p. $\square$

---

15. Use Gauss's lemma to determine whether $x^2 = 15 \pmod{17}$ has any solutions.

Gauss's lemma applies, since $(15, 17) = 1$. $\dfrac{17-1}{2} = 8$, so I compute the first 8 multiples of 15 mod 17:

k	1	2	3	4	5	6	7	8
$15k \pmod{17}$	15	13	11	9	7	5	3	1

Now $\dfrac{17}{2} = 8.5$, and 4 of these residues are greater than 8.5. By Gauss's lemma,

$$\left(\frac{15}{17}\right) = (-1)^4 = 1.$$

Therefore, $x^2 = 15 \pmod{17}$ has solutions. $\square$

---

16. Compute the following Jacobi symbols.

(a) $\left(\dfrac{37}{297}\right)$.

(b) $\left(\dfrac{175}{213}\right)$.

(a)

$$\left(\frac{37}{297}\right) = \left(\frac{37}{9 \cdot 33}\right) = \left(\frac{37}{33}\right) = \left(\frac{4}{37}\right) = 1. \quad \square$$

(b) By direct computation 3 isn't a square mod 7, so

$$\left(\frac{175}{213}\right) = \left(\frac{7 \cdot 25}{213}\right) = \left(\frac{7}{213}\right) = \left(\frac{213}{7}\right) = \left(\frac{3}{7}\right) = -1. \quad \square$$

---

17. Let p be an odd prime. Prove that

$$\left(\frac{-2}{p}\right) = \begin{cases} 1 & \text{if } p = 8k+1 \text{ or } p = 8k+3 \\ -1 & \text{if } p = 8k+5 \text{ or } p = 8k+7 \end{cases}.$$

Note for all four cases that

$$\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right) = (-1)^{(p-1)/2} \cdot (-1)^{(p^2-1)/8}.$$

If $p = 8k+1$, then

$$\frac{p-1}{2} = \frac{8k}{2} = 4k$$

$$(-1)^(- 1)^{(p-1)/2} = (-1)^{4k} = 1$$

$$\frac{p^2-1}{8} = \frac{64k^2+16k}{8} = 8k^2+2k$$

$$(-1)^{(p^2-1)/8} = 1$$

Hence, $\left(\dfrac{-2}{p}\right) = 1 \cdot 1 = 1.$

If $p = 8k + 3$, then

$$\begin{aligned} \frac{p-1}{2} &= \frac{8k+2}{2} = 4k+1 \\ (-1)^(-1)^{(p-1)/2} &= -1 \\ \frac{p^2-1}{8} &= \frac{64k^2+48k+8}{8} = 8k^2+6k+1 \\ (-1)^{(p^2-1)/8} &= -1 \end{aligned}$$

Hence, $\left(\dfrac{-2}{p}\right) = (-1) \cdot (-1) = 1.$

If $p = 8k + 5$, then

$$\begin{aligned} \frac{p-1}{2} &= \frac{8k+4}{2} = 4k+2 \\ (-1)^(-1)^{(p-1)/2} &= 1 \\ \frac{p^2-1}{8} &= \frac{64k^2+80k+24}{8} = 8k^2+10k+3 \\ (-1)^{(p^2-1)/8} &= -1 \end{aligned}$$

Hence, $\left(\dfrac{-2}{p}\right) = 1 \cdot (-1) = -1.$

If $p = 8k + 7$, then

$$\begin{aligned} \frac{p-1}{2} &= \frac{8k+6}{2} = 4k+3 \\ (-1)^(-1)^{(p-1)/2} &= -1 \\ \frac{p^2-1}{8} &= \frac{64k^2+112k+48}{8} = 8k^2+14k+6 \\ (-1)^{(p^2-1)/8} &= 1 \end{aligned}$$

Hence, $\left(\dfrac{-2}{p}\right) = (-1) \cdot 1 = -1.$ □

---

18. Convert $(7213)_8$ to base 10.

Note that

$$(7123)_8 = 7 \cdot 8^3 + 1 \cdot 8^2 + 2 \cdot 8 + 3.$$

Thus, I need to plug $x = 8$ into the polynomial $7x^3 + x^2 + 2x + 3$. I can do this, for instance, using synthetic division (Horner's method):

$$\begin{array}{r|rrrr} 8 & 7 & 2 & 1 & 3 \\ & & 56 & 464 & 3720 \\ \hline & 7 & 58 & 465 & 3723 \end{array}$$

Hence, $(7213)_8 = 3723.$ □

---

19. Convert 1808 to base 7.

I can do this by successive division by 7:

$$\begin{array}{ccccc|c} 0 & 5 & 36 & 258 & 1808 & 7 \\ & 5 & 1 & 6 & 2 & \\ \hline \end{array}$$

To see why this works, suppose that

$$1808 = a_3 \cdot 7^3 + a_2 \cdot 7^2 + a_1 \cdot 7 + a_0.$$

Rewrite the right side using Horner's method:

$$1808 = ((a_3 \cdot 7 + a_2) \cdot 7 + a_1) \cdot 7 + a_0.$$

a_0 is the remainder when 1808 is divided by 7. The quotient is $(a_3 \cdot 7 + a_2) \cdot 7 + a_1$; if I divide this quotient by 7, the remainder is a_1. And so on.

Thus, $1808 = (5162)_7$. □

---

20. Express 0.3 in base-7.

a	x	$7x$
-	0.3	2.1
2	0.1	0.7
0	0.7	4.9
4	0.9	6.3
6	0.3	2.1

For example, in the first row I multiplied 0.3 by the base 7 to get 2.1. I took the integer part of 2.1, which is 2, and put it in the first spot in the second row. Then $2.1 - 2 = 0.1$, and that goes into the second spot in the second row. Then I just repeat the process: $7 \cdot 0.1 = 0.7$, the integer part of 0.7 is 0, subtracting gives $0.7 - 0 = 0.7$, and so on. I keep going until the numbers repeat, at which point I have the expansion.

You can see why this gives the base b expansion of a number x by writing

$$x = \frac{a_0}{b} + \frac{a_1}{b^2} + \frac{a_2}{b^3} + \cdots.$$

The digits I want are a_0, a_1, and so on. Multiplying x by b gives

$$bx = a_0 + \frac{a_1}{b} + \frac{a_2}{b^2} + \cdots.$$

The integer part is a_0, and the fractional part is

$$bx - a_0 = \frac{a_1}{b} + \frac{a_2}{b^2} + \cdots.$$

Then I get a_1 by multiplying this by b, and so on.

Thus, $0.3 = (0.\overline{2046})_7$. □

---

21. Express $(0.54242\ldots)_6 = (0.5\overline{42})_6$ as a decimal fraction in lowest terms.

Let $x = (0.54242\ldots)_6$. Since the repeating part has two digits, I multiply by 6^2 to get

$$\begin{array}{r} 36x = (54.2\,4242\ldots)_6 \\ x = (\ \ 0.5\,4242\ldots)_6 \\ \hline 35x = (53.\,3)_6 \end{array}$$

Here's an explanation for the subtraction. The repeating 42's on the far right cancel. In the place to the right of the point, I'm doing 2 minus 5. As usual, I have to borrow 1 from the 4 to the left, which is where the "53" comes from. After borrowing, in the place to the right of the point, I'm doing $(12)_6 - 5_6$. This is $8 - 5 = 3$ in decimal, so the digit to the right of the point is 3.

I still have to convert $(53.3)_6$ to decimal before I solve for x:

$$(53.3)_6 = 5 \cdot 6 + 3 + 3 \cdot \frac{1}{6} = \frac{67}{2}.$$

So

$$\begin{aligned} 35x &= \frac{67}{2} \\ x &= \frac{67}{70} \quad \square \end{aligned}$$

---

22. Let b be a positive integer greater than 3. Express $(0.3(b-1)3(b-1)\ldots)_b = (0.\overline{3(b-1)})_b$ as a rational function of b.

Write the expression as an infinite series and use the formula for the sum of a geometric series:

$$(0.3(b-1)3(b-1)\ldots)_b = \frac{3}{b} + \frac{b-1}{b^2} + \frac{3}{b^3} + \frac{b-1}{b^4} + \cdots = \frac{3b + (b-1)}{b^2} + \frac{3b + (b-1)}{b^4} + \cdots =$$

$$\frac{4b-1}{b^2} + \frac{4b-1}{b^4} + \cdots = \frac{\frac{4b-1}{b^2}}{1 - \frac{1}{b^2}} = \frac{4b-1}{b^2-1}. \quad \square$$

---

23. Let b be a positive integer greater than 3. Find the base b expansion of $\dfrac{2b^2+1}{b^2-1}$.

The idea in this problem is to try to expand the expression in a power series in $\dfrac{1}{b}$. One way to do this is to make use of the geometric series

$$\frac{1}{1-x} = 1 + x + x^2 + x^3 + \cdots.$$

If $x = \dfrac{1}{b^k}$ for some k, I'll get a power series in $\dfrac{1}{b}$. So I do some algebra to get expressions of the right form.

$$\frac{2b^2+1}{b^2-1} = \frac{2 + \frac{1}{b^2}}{1 - \frac{1}{b^2}} = 2 \cdot \frac{1}{1 - \frac{1}{b^2}} + \frac{1}{b^2} \cdot \frac{1}{1 - \frac{1}{b^2}} = 2 \cdot \left(1 + \frac{1}{b^2} + \frac{1}{b^4} + \cdots\right) + \frac{1}{b^2} \cdot \left(1 + \frac{1}{b^2} + \frac{1}{b^4} + \cdots\right) =$$

$$\left(2 + \frac{2}{b^2} + \frac{2}{b^4} + \cdots\right) + \left(\frac{1}{b^2} + \frac{1}{b^4} + \frac{1}{b^6} + \cdots\right) = 2 + \frac{3}{b^2} + \frac{3}{b^4} + \frac{3}{b^6} + \cdots = (2.\overline{03})_b. \quad \square$$

24. Find the finite continued fraction expansion for $\frac{983}{237}$.

Do the Euclidean algorithm:

983	-
237	4
35	6
27	1
8	3
3	2
2	1
1	2

$$\frac{983}{237} = [4, 6, 1, 3, 2, 1, 2]. \quad \square$$

25. Find the successive convergents and the exact value of the finite continued fraction $[3, 1, 4, 1, 1, 6]$.

a	p	q	c
3	3	1	1
1	4	1	4
4	19	5	$\frac{19}{5}$
1	23	6	$\frac{23}{6}$
1	42	11	$\frac{42}{11}$
6	275	72	$\frac{275}{72}$

$$[3, 1, 4, 1, 1, 6] = \frac{275}{72}. \quad \square$$

26. Suppose x is a positive integer. Find the exact value of

$$1 + \cfrac{1}{x + \cfrac{1}{x^2 + \cfrac{1}{x^3}}}.$$

The expression is the finite continued fraction $[1, x, x^2, x^3]$.

a	p	q
1	1	1
x	$x+1$	x
x^2	$x^3 + x^2 + 1$	$x^3 + 1$
x^3	$x^6 + x^5 + x^3 + x + 1$	$x^6 + x^3 + x$

$$1 + \cfrac{1}{x + \cfrac{1}{x^2 + \cfrac{1}{x^3}}} = \frac{x^6 + x^5 + x^3 + x + 1}{x^6 + x^3 + x}. \quad \square$$

---

27. Use continued fractions to find an integer linear combination of 501 and 113 which is equal to 1.

First, find the continued fraction expansion of $\dfrac{501}{113}$:

501	-
113	4
49	2
15	3
4	3
3	1
1	3

$$\frac{501}{113} = [4, 2, 3, 3, 1, 3].$$

Next, find the convergents:

a	p	q
4	4	1
2	9	2
3	31	7
3	102	23
1	133	30
3	501	113

Finally, take the "cross product" of the p's and q's in the last two rows:

$$30 \cdot 501 + (-133) \cdot 113 = 1. \quad \square$$

To be honest, one must be inconsistent. - H. G. Wells