Math 393
10-11-2020

Review Problems for the Final

These problems are intended to help you study. The fact that a problem occurs here does not mean that there will be a similar problem on the test. And the absence of a problem from this review sheet does not mean that there won't be a problem of that kind on the test.

1. Find the coefficient of $x^{16}y^{15}$ in the expansion of $(2x^2 + y^3)^{13}$.

2. Find the number of elements of $\{1, 2, \ldots 2000\}$ which are divisible by either 8 or by 22.

3. Prove that if $n \in \mathbb{Z}^+$, then $12 \mid n^4 - n^2$.

4. Define

$$x_1 = 1, \quad x_k = 1 + x_1 x_2 \cdots x_{k-1} \quad \text{for} \quad k > 1.$$

Prove that for $n \geq 1$,

$$\sum_{k=1}^{n} \frac{1}{x_k} = 2 - \frac{1}{x_1 x_2 \cdots x_n}.$$

5. Let f_n denote the n^{th} Fibonacci number. Simplify $f_{3n+10} - f_{3n+7} - f_{3n+8}$ to a single Fibonacci number, assuming that $n \geq 0$.

6. Find all integers $n \in \mathbb{Z}^+$ such that $n + 1 \mid n^2 + 1$.

7. Find $(387, 927)$ and express it as an integer linear combination of 387 and 927.

8. Find all pairs of positive integers (m, n) such that

$$[m, n] - (m, n) = 65.$$

9. (a) Explain why the Diophantine equation $6x + 14y = 7$ has no solutions.

(b) Solve the Diophantine equation $6x + 25y = 7$.

10. Solve the Diophantine equation $x^2 + 2y^2 = 3xy + 2$.

11. Find all integer solutions (positive or negative) to the Diophantine equation $x^2 + 4y^2 = 17$.

12. Use Fermat factorization to factor 43621.

13. Solve the system of congruences

$$\begin{aligned} x &= 6 \pmod{12} \\ x &= 3 \pmod{5} \\ x &= 4 \pmod{11} \end{aligned} \; .$$

14. Solve $3x + 4y = 7 \pmod{8}$. Include ranges for the parameters which give all the distinct solutions mod 8, without duplication.

15. If n is an integer, can $n^4 + n^2 + 1$ be divisible by 5?

16. Prove that if $x = a \pmod{b}$, $x = a \pmod{c}$, and $(b, c) = 1$, then $x = a \pmod{bc}$.

17. (a) List the numbers in $\{0, 1, 2, 3, 4, 5, 6, 7, 8\}$ which are invertible mod 9.

(b) A number $u \in \{0, 1, \ldots, n-1\}$ which is invertible mod n is a **primitive root** mod n if the powers u, u^2, u^3, ... of u give all the numbers which are invertible mod n. Show that 2 is a primitive root mod 9.

(c) Show by computation that there is no primitive root mod 8.

18. 2063 and 3041 are primes. Prove without computation that

$$2063^{3040} + 3041^{2062} = 1 \pmod{2063 \cdot 3041}.$$

19. Reduce $\dfrac{5062!}{5002!}$ mod 61 to a number in the range $\{0, 1, \ldots, 60\}$.

20. Solve the system of congruences

$$\begin{array}{rcrcl} 2x & + & 3y & = & 4 \pmod 5 \\ x & + & 2y & = & 3 \pmod 5 \end{array}.$$

21. Compute $\phi(864)$, $\sigma(864)$, and $\tau(864)$.

22. Calvin Butterball says: "If $n > 1$, the factors of n come in pairs $\{a, b\}$, where $n = ab$. Hence, $\tau(n)$ must be even." Is he right?

23. For what positive integers n does $\phi(5n) = 5\phi(n)$?

24. Let $n \geq 2$. Consider the set S of integers in $\{1, 2, \ldots, n-1\}$ which are relatively prime to n. Prove that the sum of the elements of S is $\dfrac{n \cdot \phi(n)}{2}$.

25. Find the last three digits of 7^{8403}.

26. Show that if $\sigma(n) = 36$, then $n = 22$.

27. Prove that if n is an integer and $3 \not| n$, then $n^{37} - n$ is divisible by 54.

28. Show that $2^{31} - 1$ has no prime factors less than 500.

29. Find the decoding transformation for the block cipher

$$\begin{bmatrix} c_1 \\ c_2 \end{bmatrix} = \begin{bmatrix} 17 & 3 \\ 5 & 2 \end{bmatrix} \begin{bmatrix} p_1 \\ p_2 \end{bmatrix} \pmod{26}.$$

30. Consider the exponential cipher which uses the prime $p = 3121$ and the exponent $e = 11$.

(a) Encipher the word FOOD.

(b) Find the deciphering transformation.

31. For an RSA cipher, it is known that the modulus is $n = 240181$, and $\phi(240181) = 239200$. Find the primes p and q such that $n = pq$.

32. Find all solutions to the congruence

$$x^2 = 74 \pmod{203}.$$

Note: $203 = 7 \cdot 29$.

33. Find a solution to $x^2 = 208 \pmod{289}$ by lifting a solution to the congruence mod 17.

34. Suppose that p is an odd prime and $p = 19 \pmod{20}$. Compute $\left(\dfrac{-5}{p}\right)$.

35. Compute $\left(\dfrac{180}{211}\right)$.

36. Compute $\left(\dfrac{375}{461}\right)$.

37. Convert $(5573)_6$ to base 10.

38. Convert 2781 to base 5.

39. Express 0.26 in base 5.

40. Find a decimal fraction in lowest terms equal to $(0.2\overline{56})_7$.

41. Express $(.1\overline{25})_6$ as a decimal fraction in lowest terms.

42. If b is an integer and $b > 1$, find a decimal fraction equal to $(0.\overline{1})_b$.

43. Find the finite continued fraction expansion for $\dfrac{271}{43}$.

44. (a) Find the first 5 convergents of $[7; \overline{5, 10}]$.

(b) Find the exact value of $x = [7; \overline{5, 10}]$.

45. Find the first 10 terms of the continued fraction expansion of $\sqrt[3]{114}$.

46. (a) Find the continued fraction expansion of $\sqrt{7}$. Find the convergents c_0, ..., c_8.

(b) Use the convergents of the continued fraction expansion of $\sqrt{7}$ to find a solution to the Fermat-Pell equation $x^2 - 7y^2 = 1$.

47. Find the convergents of the finite continued fraction $[1; 1, 4, 1, 4, 1, 4]$.

48. Find the exact value of the periodic continued fraction $[1; \overline{2, 5}]$.

49. Find the rational number $\dfrac{p}{q}$ in lowest terms with $q \le 50$ which best approximates $\dfrac{\pi}{e}$.

Solutions to the Review Problems for the Final

1. Find the coefficient of $x^{16}y^{15}$ in the expansion of $(2x^2 + y^3)^{13}$.

I'll get a $x^{16}y^{15}$ term by taking $(2x^2)^8$ and $(y^3)^5$. Thus, the coefficient is $\binom{13}{8} \cdot 2^8 = 329472$. $\square$

---

2. Find the number of elements of $\{1, 2, \ldots 2000\}$ which are divisible by either 8 or by 22.

The number of elements of $\{1, 2, \ldots 2000\}$ which are divisible by 8 is

$$\left[\frac{2000}{8}\right] = 250.$$

The number of elements of $\{1, 2, \ldots 2000\}$ which are divisible by 22 is

$$\left[\frac{2000}{22}\right] = [90.90909\ldots] = 90.$$

The number of elements of $\{1, 2, \ldots 2000\}$ which are divisible by both 8 and 22 is the number divisible by their least common multiple, and $[8, 22] = 88$. The number of elements of $\{1, 2, \ldots 2000\}$ which are divisible by 88 is

$$[2000 88] = [22.72727\ldots] = 22.$$

The number divisible by both is counted in both the number divisible by 8 and the number divisible by 22. So it must be subtracted off once to get the number divisible by either 8 or 22:

$$250 + 90 - 22 = 318. \quad \square$$

---

3. Prove that if $n \in \mathbb{Z}^+$, then $12 \mid n^4 - n^2$.

For $n = 1$, I have $n^4 - n^2 = 1^4 - 1^2 = 0$, and $12 \mid 0$.
Suppose $12 \mid n^4 - n^2$. I want to show that $12 \mid (n+1)^4 - (n+1)^2$. Now

$$\begin{aligned} (n+1)^4 - (n+1)^2 &= (n^4 + 4n^3 + 6n^2 + 4n + 1) - (n^2 + 2n + 1) \\ &= (n^4 - n^2) + (4n^3 + 6n^2 + 2n) \\ &= (n^4 - n^2) + 2n(2n^2 + 3n + 1) \\ &= (n^4 - n^2) + 2n(n+1)(2n+1) \end{aligned}$$

I know that $12 \mid n^4 - n^2$ by induction.
To show that $12 \mid 2n(n+1)(2n+1)$, you can take several approaches. One approach is to consider $n = 0, 1, \ldots, 11$ mod 12 and show that you always get 0. A sneakier approach is to note that

$$\begin{aligned} 1^2 + 2^2 + 3^2 + \cdots + n^2 &= \frac{n(n+1)(2n+1)}{6} \\ 12(1^2 + 2^2 + 3^2 + \cdots + n^2) &= 2n(n+1)(2n+1) \end{aligned}$$

In any event, since $12 \mid n^4 - n^2$ and $12 \mid 2n(n+1)(2n+1)$, I have $12 \mid (n+1)^4 - (n+1)^2$. This completes the induction step and the proof. $\square$

---

4. Define

$$x_1 = 1, \quad x_k = 1 + x_1 x_2 \cdots x_{k-1} \quad \text{for} \quad k > 1.$$

Prove that for $n \geq 1$,

$$\sum_{k=1}^{n} \frac{1}{x_k} = 2 - \frac{1}{x_1 x_2 \cdots x_n}.$$

For $n = 1$,

$$\sum_{k=1}^{1} \frac{1}{x_k} = \frac{1}{x_1} = \frac{1}{1} = 1,$$

$$2 - \frac{1}{x_1} = 2 - \frac{1}{1} = 1.$$

The result is true for $n = 1$.
Let $n > 1$, and assume that the result holds for $n - 1$:

$$\sum_{k=1}^{n-1} \frac{1}{x_k} = 2 - \frac{1}{x_1 x_2 \cdots x_{n-1}}.$$

Then

$$\sum_{k=1}^{n} \frac{1}{x_k} = \sum_{k=1}^{n-1} \frac{1}{x_k} + \frac{1}{x_n} = 2 - \frac{1}{x_1 x_2 \cdots x_{n-1}} + \frac{1}{x_n} =$$

$$2 - \frac{x_n - x_1 x_2 \cdots x_{n-1}}{x_1 x_2 \cdots x_{n-1} x_n} = 2 - \frac{1}{x_1 x_2 \cdots x_{n-1} x_n}.$$

(The second equality used the induction hypothesis, the third equality came from combining fractions over a common denominator, and the fourth equality came from the definition of the x's.)

Therefore, the result holds for n, so it's true for all $n \geq 1$, by induction. $\square$

---

5. Let f_n denote the n^{th} Fibonacci number. Simplify $f_{3n+10} - f_{3n+7} - f_{3n+8}$ to a single Fibonacci number, assuming that $n \geq 0$.

$$f_{3n+10} - f_{3n+7} - f_{3n+8} = f_{3n+10} - (f_{3n+7} + f_{3n+8}) = f_{3n+10} - f_{3n+9} = f_{3n+8}. \quad \square$$

---

6. Find all integers $n \in \mathbb{Z}^+$ such that $n + 1 \mid n^2 + 1$.

Suppose $n + 1 \mid n^2 + 1$. Then

$$n + 1 \mid n^2 + 1 = (n^2 + 2n + 1) - 2n = (n + 1)^2 - 2n.$$

But $n + 1 \mid (n + 1)^2$, so $n + 1 \mid 2n$.
Say $k(n + 1) = 2n$, where $k \in \mathbb{Z}^+$. If $k \geq 2$, then

$$\begin{aligned} k(n+1) &\geq 2(n+1) \\ 2n &\geq 2(n+1) \\ 2n &\geq 2(n+1) > 2n \end{aligned}$$

This is a contradiction. Hence, $k = 1$. This means that $1(n + 1) = 2n$, so $n = 1$. $\square$

---

7. Find $(387, 927)$ and express it as an integer linear combination of 387 and 927.

927	-	12
387	2	5
153	2	2
81	1	1
72	1	1
9	8	0

$$(-5)(927) + (12)(387) = 9 = (387, 927). \quad \square$$

---

8. Find all pairs of positive integers (m, n) such that

$$[m, n] - (m, n) = 65.$$

Note that $(m, n) \mid m \mid [m, n]$. Hence,

$$(m, n) \mid [m, n] - (m, n) = 65.$$

Now 65 has 4 positive divisors: 1, 5, 13, and 65. I consider each of these cases.

Case 1. $(m, n) = 1$.

Using $[m, n] = \dfrac{mn}{(m, n)}$, I get $[m, n] = mn$. So

$$\begin{aligned}
[m, n] - (m, n) &= 65 \\
mn - 1 &= 65 \\
mn &= 66
\end{aligned}$$

m and n are relatively prime ($(m, n) = 1$) positive integers whose product is 66. This gives me the following pairs (ignoring order):

$$(m, n) = (1, 66), \quad (2, 33), \quad (3, 22), \quad (6, 11).$$

Case 2. $(m, n) = 5$.

$(m, n) \mid m$, so $m = (m, n)a = 5a$. Likewise, $(m, n) \mid n$, so $n = (m, n)b = 5b$. Since I've divided m and n by their greatest common divisor, I must have $(a, b) = 1$.

Moreover,

$$[m, n] = \frac{mn}{(m, n)} = \frac{(5a)(5b)}{5} = 5ab.$$

So

$$\begin{aligned}
[m, n] - (m, n) &= 65 \\
5ab - 5 &= 65 \\
5ab &= 70 \\
ab &= 14
\end{aligned}$$

a and b are relatively prime positive integers whose product is 14. This gives me the following pairs (ignoring order):

$$(a, b) = (1, 14), \quad (2, 7).$$

If $(a, b) = (1, 14)$, then multiplying by 5 gives $(m, n) = (5, 70)$.

If $(a, b) = (2, 7)$, then multiplying by 5 gives $(m, n) = (10, 35)$.

Case 3. $(m, n) = 13$.

$(m, n) \mid m$, so $m = (m, n)a = 13a$. Likewise, $(m, n) \mid n$, so $n = (m, n)b = 13b$. Since I've divided m and n by their greatest common divisor, I must have $(a, b) = 1$.

Moreover,

$$[m, n] = \frac{mn}{(m, n)} = \frac{(13a)(13b)}{13} = 13ab.$$

So

$$\begin{aligned}
[m, n] - (m, n) &= 65 \\
13ab - 13 &= 65 \\
13ab &= 78 \\
ab &= 6
\end{aligned}$$

a and b are relatively prime positive integers whose product is 6. This gives me the following pairs (ignoring order):

$$(a, b) = (1, 6), \quad (2, 3).$$

If $(a,b) = (1,6)$, then multiplying by 13 gives $(m,n) = (13,78)$.
If $(a,b) = (2,3)$, then multiplying by 13 gives $(m,n) = (26,39)$.

Case 4. $(m,n) = 65$.

$(m,n) \mid m$, so $m = (m,n)a = 65a$. Likewise, $(m,n) \mid n$, so $n = (m,n)b = 65b$. Since I've divided m and n by their greatest common divisor, I must have $(a,b) = 1$.

Moreover,

$$[m,n] = \frac{mn}{(m,n)} = \frac{(65a)(65b)}{65} = 65ab.$$

So

$$\begin{aligned}
[m,n] - (m,n) &= 65 \\
65ab - 65 &= 65 \\
65ab &= 130 \\
ab &= 2
\end{aligned}$$

a and b are relatively prime positive integers whose product is 2. The only solution (ignoring order) is $(a,b) = (1,2)$.

If $(a,b) = (1,2)$, then multiplying by 65 gives $(m,n) = (65,130)$.

All together, the solutions are:

$$(m,n) = (1,66),\quad (2,33),\quad (3,22),\quad (6,11),\quad (5,70),\quad (10,35),\quad (13,78),\quad (26,39),\quad (65,130). \quad \square$$

---

9. (a) Explain why the Diophantine equation $6x + 14y = 7$ has no solutions.

(b) Solve the Diophantine equation $6x + 25y = 7$.

(a) If (x,y) is a solution, then $2 \mid 6x + 14y$, but $2 \not| 7$, contradicting the fact that $6x + 14y = 7$. $\square$

(b) $(6,25) = 1 \mid 7$, so there are solutions.

I could find a particular solution by inspection; instead, I'll do it systematically using the Extended Euclidean algorithm.

25	-	4
6	4	1
1	6	0

Thus,

$$(6)(-4) + (25)(1) = 1.$$

Multiply by 7:

$$(6)(-28) + (25)(7) = 7.$$

Thus, $x_0 = -28$, $y_0 = 7$ is a particular solution. The general solution is

$$x = -28 + 25s, \quad y = 7 - 6s. \quad \square$$

---

10. Solve the Diophantine equation $x^2 + 2y^2 = 3xy + 2$.

Rewrite the equation as

$$x^2 - 3xy + 2y^2 = 3, \quad \text{or} \quad (x-y)(x-2y) = 2.$$

There are 4 possibilities, corresponding to the four ways of factoring 2 into a product of 2 integers.

Case 1: $x - y = 1$ and $x - 2y = 2$.

Adding the equations gives $y = -1$, and so $x = 0$.

Case 2: $x - y = 2$ and $x - 2y = 1$.

Adding the equations gives $y = 1$, and so $x = 3$.

Case 3: $x - y = -1$ and $x - 2y = -2$.

Adding the equations gives $y = 1$, and so $x = 0$.

Case 4: $x - y = -2$ and $x - 2y = -1$.

Adding the equations gives $y = -1$, and so $x = -1$.

The solutions are $(0, -1)$, $(3, 1)$, $(0, 1)$, and $(-1, -1)$. $\square$

---

11. Find all integer solutions (positive or negative) to the Diophantine equation $x^2 + 4y^2 = 17$.

Note that $|x| < \sqrt{17}$ and $|y| < \dfrac{\sqrt{17}}{2}$, so I can simply check cases. Note also that $4y^2$ is even and 17 is odd, so x^2 must be odd, and hence x must be odd. Finally, if x works, so does $-x$, and likewise for y and $-y$. Therefore, I only need to check positive numbers.

Putting all these constraints together, I find that I only need to try $x = 1$ and $x = 3$.

If $x = 1$, then $4y^2 = 17 - x^2 = 16$, so $y = \pm 2$. This gives the four solutions $(1, 2)$, $(1, -2)$, $(-1, 2)$, $(-1, -2)$.

If $x = 3$, then $4y^2 = 17 - 9 = 8$. This has no integer solutions.

The only solutions are $(1, 2)$, $(1, -2)$, $(-1, 2)$, $(-1, -2)$. $\square$

---

12. Use Fermat factorization to factor 43621.

Since $\sqrt{43621} \approx 208.85641$, I'll start at $n = 209$.

n	$n^2 - 43621$	$\sqrt{n^2 - 43621}$
209	60	7.74596...
210	479	21.88606...
211	900	30

I have

$$\begin{aligned} 30^2 &= 211^2 - 43621 \\ 43621 &= 211^2 - 30^2 \\ 43621 &= (211 + 30)(211 - 30) \\ 43621 &= 241 \cdot 181 \end{aligned}$$

You can check that 241 and 181 are prime. $\square$

---

13. Solve the system of congruences

$$\begin{aligned} x &= 6 \pmod{12} \\ x &= 3 \pmod{5} \\ x &= 4 \pmod{11} \end{aligned} .$$

The moduli are relatively prime. The Chinese Remainder Theorem implies that there is a unique solution mod $12 \cdot 5 \cdot 11 = 660$.

$x = 6 \pmod{12}$ implies that $x = 6 + 12s$. So

$$\begin{aligned} 6 + 12s &= 3 \pmod{5} \\ 1 + 2s &= 3 \pmod{5} \\ 2s &= 2 \pmod{5} \\ s &= 1 \pmod{5} \end{aligned}$$

This means that $s = 1 + 5t$, so

$$x = 6 + 12(1 + 5t) = 18 + 60t.$$

Then

$$\begin{aligned} 18 + 60t &= 4 \pmod{11} \\ 7 + 5t &= 4 \pmod{11} \\ 5t &= 8 \pmod{11} \\ t &= 6 \pmod{11} \end{aligned}$$

This means that $t = 6 + 11u$, so

$$x = 18 + 60(6 + 11u) = 378 + 660u.$$

Therefore, $x = 378 \pmod{660}$. $\square$

---

14. Solve $3x + 4y = 7 \pmod{8}$. Include ranges for the parameters which give all the distinct solutions mod 8, without duplication.

Since $(3, 4, 8) = 1 \mid 7$, there are $1 \cdot 8 = 8$ distinct solutions mod 8.
Write the congruence as the Diophantine equation

$$3x + 4y + 8z = 7.$$

Let $w = 3x + 4y$. Then

$$w + 8z = 7.$$

By inspection, $w_0 = -1$, $z_0 = 1$ is a particular solution. The general solution is

$$w = -1 + 8s, \quad z = 1 - s.$$

Therefore,

$$-1 + 8s = 3x + 4y.$$

By inspection, $x_0 = 1$, $y_0 = -1 + 2s$ is a particular solution. The general solution is

$$x = 1 + 4t, \quad y = -1 + 2s - 3t.$$

Reducing mod 8,

$$x = 1 + 4t \pmod{8}, \quad y = 7 + 2s + 5t \pmod{8}.$$

The parameter ranges $t = 0, 1,\ s = 0, 1, 2, 3$ give the 8 distinct solutions:

t	s	x	y
0	0	1	7
0	1	1	1
0	2	1	3
0	3	1	5
1	0	5	4
1	1	5	6
1	2	5	0
1	3	5	2

$\square$

---

15. If n is an integer, can $n^4 + n^2 + 1$ be divisible by 5?

$n \pmod 5$	0	1	2	3	4
$n^4 + n^2 + 1 \pmod 5$	1	3	1	1	3

The table shows that for all n, $n^4 + n^2 + 1 \neq 0 \pmod 5$. Therefore, $n^4 + n^2 + 1$ is never divisible by 5. $\square$

---

16. Prove that if $x = a \pmod b$, $x = a \pmod c$, and $(b, c) = 1$, then $x = a \pmod{bc}$.

$x = a \pmod b$ means that $b \mid x - a$ and $x = a \pmod c$ means that $c \mid x - a$. Also, $(b, c) = 1$ implies that

$$bm + cn = 1 \quad \text{for some} \quad m, n.$$

Multiply by $x - a$:

$$bm(x - a) + cn(x - a) = x - a.$$

$b \mid b$ and $c \mid x - a$ imply that $bc \mid bm(x - a)$. Also, $c \mid c$ and $b \mid x - a$ imply that $bc \mid cn(x - a)$. Thus,

$$bc \mid bm(x - a) + cn(x - a) = x - a.$$

Hence, $x = a \pmod{bc}$. $\square$

---

17. (a) List the numbers in $\{0, 1, 2, 3, 4, 5, 6, 7, 8\}$ which are invertible mod 9.

(b) A number $u \in \{0, 1, \ldots, n - 1\}$ which is invertible mod n is a **primitive root** mod n if the powers u, u^2, u^3, ... of u give all the numbers which are invertible mod n. Show that 2 is a primitive root mod 9.

(c) Show by computation that there is no primitive root mod 8.

(a) The numbers which are invertible mod 9 are those which are relatively prime to 9:

$$1, \quad 2, \quad 4, \quad 5, \quad 7, \quad 8. \quad \square$$

(b)

$$2^1 = 2, \quad 2^2 = 4, \quad 2^3 = 8, \quad 2^4 = 7, \quad 2^5 = 5, \quad 2^6 = 1.$$

I've gotten all of the numbers in $\{1, 2, 4, 5, 7, 8\}$ by taking powers of 2, so 2 is a primitive root mod 9. $\square$

(c) The numbers in $\{0, 1, 2, 3, 4, 5, 6, 7\}$ which are invertible mod 8 are 1, 3, 5, and 7. However,

$$1^2 = 1 \pmod{8}, \quad 3^2 = 1 \pmod{8}, \quad 5^2 = 1 \pmod{8}, \quad 7^2 = 1 \pmod{8}.$$

Therefore, you can't get all four of 1, 3, 5, and 7 by taking powers of any of these elements. Hence, there is no primitive root mod 8. $\square$

Note: If $n \in \mathbb{Z}^+$, then n has a primitive root if and only if $n = 1, 2, 4, p^k, 2p^k$, where p is an odd prime.

---

18. 2063 and 3041 are primes. Prove without computation that

$$2063^{3040} + 3041^{2062} = 1 \pmod{2063 \cdot 3041}.$$

By Fermat's theorem with the prime 3041,

$$2063^{3040} = 1 \pmod{3041}, \quad \text{so} \quad 2063^{3040} + 3041^{2062} = 1 \pmod{3041}.$$

By Fermat's theorem with the prime 2063,

$$3041^{2062} = 1 \pmod{2063}, \quad \text{so} \quad 2063^{3040} + 3041^{2062} = 1 \pmod{2063}.$$

Since 2063 and 3041 are distinct primes, they're relatively prime. Hence,

$$2063^{3040} + 3041^{2062} = 1 \pmod{2063 \cdot 3041}.$$

Remark: This result is true with any two distinct primes in place of 2063 and 3041. $\square$

---

19. Reduce $\dfrac{5062!}{5002!}$ mod 61 to a number in the range $\{0, 1, \ldots, 60\}$.

$$\frac{5062!}{5002!} = 5003 \cdot 5004 \cdots 5062.$$

Since $82 \cdot 61 = 5002$ and $83 \cdot 61 = 5063$, the numbers 5003, 5004, ..., 5062 must reduce mod 61 to 1, 2, ..., 60. By Wilson's theorem,

$$\frac{5062!}{5002!} = 5003 \cdot 5004 \cdots 5062 = 1 \cdot 2 \cdots 60 = 60! = -1 = 60 \pmod{61}. \quad \square$$

---

20. Solve the system of congruences

$$\begin{array}{ccccc} 2x & + & 3y & = & 4 \pmod{5} \\ x & + & 2y & = & 3 \pmod{5} \end{array}.$$

Write the system in matrix form:

$$\begin{bmatrix} 2 & 3 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 4 \\ 3 \end{bmatrix} \pmod{5}.$$

Solve the system by inverting the coefficient matrix:

$$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 2 & 3 \\ 1 & 2 \end{bmatrix}^{-1} \begin{bmatrix} 4 \\ 3 \end{bmatrix} = \frac{1}{1} \cdot \begin{bmatrix} 2 & 2 \\ 4 & 2 \end{bmatrix} \begin{bmatrix} 4 \\ 3 \end{bmatrix} = \begin{bmatrix} 4 \\ 2 \end{bmatrix} \pmod{5}. \quad \square$$

Note: You can also solve using Cramer's rule or row reduction. Or you can solve the second equation to get $x = 3y + 3 \pmod{5}$, and plug this into the first equation and solve for y.

---

21. Compute $\phi(864)$, $\sigma(864)$, and $\tau(864)$

$864 = 2^5 \cdot 3^3$, so

$$\phi(864) = 864 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) = 288,$$

$$\sigma(864) = \left(\frac{2^6 - 1}{2 - 1}\right) \left(\frac{3^4 - 1}{3 - 1}\right) = (63)(40) = 2520,$$

$$\tau(864) = (5 + 1)(3 + 1) = 24. \quad \square$$

---

22. Calvin Butterball says: "If $n > 1$, the factors of n come in pairs $\{a, b\}$, where $n = ab$. Hence, $\tau(n)$ must be even." Is he right?

Calvin is forgetting that a and b could be equal. In fact, $\tau(n)$ is even *provided that* n is not a perfect square; otherwise, $\tau(n)$ is odd. (Try writing a careful proof of this.) For example $\tau(4) = 3$. $\square$

---

23. For what positive integers n does $\phi(5n) = 5\phi(n)$?

If $5 \nmid n$, then $(n, 5) = 1$, so

$$\phi(5n) = \phi(5)\phi(n) = 4\phi(n) \neq 5\phi(n).$$

On the other hand, suppose $5 \mid n$. I can write $n = 5^k m$, where $k \geq 1$ and $(m, 5) = 1$. Then

$$5\phi(n) = 5\phi(5^k m) = 5\phi(5^k)\phi(m) = 5(5^k - 5^{k-1})\phi(m) = (5^{k+1} - 5^k)\phi(m),$$

$$\phi(5n) = \phi(5^{k+1} m) = \phi(5^{k+1})\phi(m) = (5^{k+1} - 5^k)\phi(m).$$

Therefore, $5\phi(n) = \phi(5n)$.
Hence, $\phi(5n) = 5\phi(n)$ if and only if $5 \mid n$. $\square$

---

24. Let $n \geq 2$. Consider the set S of integers in $\{1, 2, \ldots, n-1\}$ which are relatively prime to n. Prove that the sum of the elements of S is $\dfrac{n \cdot \phi(n)}{2}$.

The case $n = 2$ can be proved directly: The only positive integer in $\{1\}$ relatively prime to 2 is 1, and $\dfrac{2 \cdot \phi(2)}{2} = 1$.
So assume $n > 2$.
First, note that if $m \in S$, then $n - m \in S$. For

$$(m, n) = (m, n - m) = (m + (n - m), n - m) = (n, n - m).$$

Thus, $(m, n) = 1$ if and only if $(n - m, n) = 1$.

This means that the integers in S occur in pairs $\{m, n-m\}$.

I claim that that the elements of such a pair are distinct. Suppose on the contrary that $m = n - m$, so $m = \dfrac{n}{2}$.

If n is odd, then $\dfrac{n}{2}$ is not an integer, but m is, and I have a contradiction.

If n is even, then $\dfrac{n}{2}$ is an integer that divides n (since $2 \cdot \dfrac{n}{2} = n$). Moreover, since $n > 2$, I have $\dfrac{n}{2} > 1$. This means that $\left(\dfrac{n}{2}, n\right) = \dfrac{n}{2} \neq 1$, so $m = \dfrac{n}{2} \notin S$, another contradiction.

Thus, S can be broken down into pairs $(m, n-m)$. The sum of the two elements in each pair is $m + (n - m) = n$. Since $|S| = \phi(n)$, there must be $\dfrac{\phi(n)}{2}$ pairs. Therefore, the sum of the elements of S is $n \cdot \dfrac{\phi(n)}{2}$, as I wanted to show. $\square$

---

25. Find the last three digits of 7^{8403}.

$\phi(1000) = 400$, so by Euler's theorem,

$$7^{8403} = (7^{400})^21 \cdot 7^3 = 1^{21} \cdot 343 = 343 \pmod{1000}.$$

The last three digits of 7^{8403} are 343. $\square$

---

26. Show that if $\sigma(n) = 36$, then $n = 22$.

Write the prime factorization of n:

$$n = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}.$$

Then

$$\sigma(n) = (1 + p_1 + \cdots + p_1^{r_1})(1 + p_2 + \cdots + p_2^{r_2}) \cdots (1 + p_k + \cdots + p_k^{r_k}).$$

Here is a table of values of $1 + p + \cdots + p^n$ for various primes p:

	$n = 1$	$n = 2$	$n = 3$	$n = 4$	$n = 5$
$p = 2$	3	7	15	31	63
$p = 3$	4	13	40	121	364
$p = 5$	6	31	156	781	3906
$p = 7$	8	57	400	2801	19608
$p = 11$	12	133	1464	16105	177156
$p = 13$	14	183	2380	30941	402234
$p = 17$	18	307	5220	88741	1508598
$p = 19$	20	381	7240	137561	2613660

Note that 36 does not occur in the first column, since $36 - 1 = 35$ is not prime. Clearly, the numbers in each row and column increase. Thus, any factors of 36 that *could* occur must be in the table.

The divisors of 36 that occur in the table are 3, 4, 6, 12, and 18.

18 can't be part of the factorization of $\sigma(n) = 36$, since I don't have any way of getting a factor of 2.

6 can't be part of the factorization, since I can only get the remaining factor of 6 as 6 or as $2 \cdot 3$. I can't use 6 a second time, and I can't get a factor of 2.

4 can't be part of the factorization, since I can only get the remaining factor of 9 as 9 or as $3 \cdot 3$. There is no 9 in the table, and I can't use 3 twice.

The only possibility is that $\sigma(n) = 3 \cdot 12$; consulting the table, this means that $n = 2 \cdot 11 = 22$. $\square$

---

27. Prove that if n is an integer and $3 \nmid n$, then $n^{37} - n$ is divisible by 54.

To say that $n^{37} - n$ is divisible by 54 is the same as saying that $n^{37} = n \pmod{54}$. Since $54 = 2 \cdot 27$ and $(2, 27) = 1$, it suffices to prove that $n^{37} = n \pmod{2}$ and $n^{37} = n \pmod{27}$.

Since 2 is prime, $n^2 = n \pmod{2}$ by a corollary to Fermat's theorem.

$(n, 27) \mid 27$, so $(n, 27) = 1, 3, 9, 27$. If $(n, 27) \neq 1$, then $3 \mid (n, 27) \mid n$, which contradicts the assumption that $3 \nmid n$. Therefore, $(n, 27) = 1$.

Hence, I may apply Euler's theorem: $\phi(27) = 18$, so $n^{18} = 1 \pmod{27}$. Then

$$n^{36} = 1 \pmod{27}, \quad \text{and} \quad n^{37} = n \pmod{27}.$$

Since $n^2 = n \pmod{2}$ and $n^{37} = n \pmod{27}$, it follows that $n^{37} = n \pmod{54}$.

Note that the result may not hold if $3 \mid n$. For example, $9^{37} - 9 = 18 \pmod{54}$. $\square$

---

28. Convert $(5573)_6$ to base 10.

$$\begin{array}{c|cccc} 6 & 5 & 5 & 7 & 3 \\ & & 30 & 210 & 1302 \\ \hline & 5 & 35 & 217 & 1305 \end{array}$$

Hence, $(5573)_6 = 1305$. $\square$

---

29. Show that $2^{31} - 1$ has no prime factors less than 500.

Since 31 is prime, divisors of $2^{31} - 1$ have the form $2 \cdot 31k + 1 = 62k + 1$. I check numbers of this form less than 500:

n	$62n + 1$	Result
1	63	63 isn't prime
2	125	125 isn't prime
3	187	187 isn't prime
4	249	249 isn't prime
5	311	$311 \nmid 2^{31} - 1$
6	373	$373 \nmid 2^{31} - 1$
7	435	435 isn't prime
8	497	497 isn't prime

Thus, $2^{31} - 1$ has no prime factors less than 500. In fact, $2^{31} - 1$ is prime. $\square$

---

30. Find the decoding transformation for the block cipher

$$\begin{bmatrix} c_1 \\ c_2 \end{bmatrix} = \begin{bmatrix} 17 & 3 \\ 5 & 2 \end{bmatrix} \begin{bmatrix} p_1 \\ p_2 \end{bmatrix} \pmod{26}.$$

The determinant of the coefficient matrix is $17 \cdot 2 - 3 \cdot 5 = 19$, and $(19, 26) = 1$. Hence, the matrix is invertible.

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

$$\begin{aligned} (-8) \cdot 26 + 11 \cdot 19 &= 1 \\ 11 \cdot 19 &= 1 \pmod{26} \end{aligned}$$

Hence, $19^{-1} = 11 \pmod{26}$.
Therefore,

$$\begin{bmatrix} 17 & 3 \\ 5 & 2 \end{bmatrix}^{-1} = 11 \cdot \begin{bmatrix} 2 & -33 \\ -5 & 17 \end{bmatrix} = \begin{bmatrix} 22 & -343 \\ -55 & 187 \end{bmatrix} = \begin{bmatrix} 22 & 21 \\ 23 & 5 \end{bmatrix}.$$

The decoding transformation is

$$\begin{bmatrix} p_1 \\ p_2 \end{bmatrix} = \begin{bmatrix} 22 & 21 \\ 23 & 5 \end{bmatrix} \begin{bmatrix} c_1 \\ c_2 \end{bmatrix} \pmod{26}. \quad \square$$

---

31. Consider the exponential cipher which uses the prime $p = 3121$ and the exponent $e = 11$.

(a) Encipher the word FOOD.

(b) Find the deciphering transformation.

(a) Since $2525 < 3121 < 252525$, I use blocks of two letters. FOOD becomes 0514 1403.

I'll do the first block by way of example. I'll do the computation the way you would do it on a calculator which can't accomodate very big numbers.

$$514^{11} = (514^3)^3(514^2) = (2034)^3(2032) = (2034^2)(2034 \cdot 2032) = (1831)(884) = 1926 \pmod{3121}$$

.

Similarly,

$$1403^{11} = 592 \pmod{3121}.$$

The ciphertext is 1926 0592. $\square$

(b) I need d such that $de = 1 \pmod{3120}$, i.e. such that $11d = 1 \pmod{3120}$. Use the Extended Euclidean algorithm:

3120	-	851
11	283	3
7	1	2
4	1	1
3	1	1
1	3	0

Thus,

$$(-3)(3120) + (851)(11) = 1 \pmod{3120}, \quad \text{or} \quad (851)(11) = 1 \pmod{3120}.$$

Thus, $d = 851$, and the decoding transformation is

$$P = C^{851} \pmod{3121}. \quad \square$$

---

32. For an RSA cipher, it is known that the modulus is $n = 240181$, and $\phi(240181) = 239200$. Find the primes p and q such that $n = pq$.

Note that

$$\phi(n) = \phi(pq) = (p-1)(q-1) = pq - p - q + 1 = n - (p+q) + 1.$$

Thus,

$$p + q = n - \phi(n) + 1 = 240181 - 239200 + 1 = 982.$$

Next,

$$(p-q)^2 = p^2 - 2pq + q^2 = (p^2 + 2pq + q^2) - 4pq = (p+q)^2 - 4n.$$

Hence,

$$p - q = \sqrt{(p+q)^2 - 4n} = \sqrt{982^2 - 4 \cdot 240181} = 60.$$

Then

$$p = \frac{1}{2}\left((p+q) + (p-q)\right) = \frac{1}{2}(982 + 60) = 521,$$
$$q = \frac{1}{2}\left((p+q) - (p-q)\right) = \frac{1}{2}(982 - 60) = 461. \quad \square$$

---

33. Find all solutions to the congruence

$$x^2 = 74 \pmod{203}.$$

Note: $203 = 7 \cdot 29$.

I'll begin by solving the congruence mod 7 and mod 29.

$$x^2 = 74 = 4 \pmod{7}.$$

The solutions are obviously $x = 2 \pmod{7}$ and $x = -2 = 5 \pmod{7}$.

$$x^2 = 74 = 16 \pmod{29}.$$

The solutions are obviously $x = 4 \pmod{29}$ and $x = -4 = 25 \pmod{29}$.

(In cases where you couldn't find solutions to these by inspection, you'd probably need to make a table of squares.)

Next, I combine solutions mod 7 with solutions mod 29 using the Chinese Remainder theorem.

First,

$$x = 2 \pmod{7}$$
$$x = 4 \pmod{29}$$

m	7	29
p	29	7
s	$1^{-1} = 1 \pmod{7}$	$7^{-1} = 25 \pmod{29}$
a	2	4

$$x = 29 \cdot 1 \cdot 2 + 7 \cdot 25 \cdot 4 = 758 = 149 \pmod{203}.$$

Hence, $x = -149 = 54 \pmod{203}$ is another solution.

Next,

$$\begin{aligned} x &= 2 \pmod{7} \\ x &= 25 \pmod{29} \end{aligned}$$

Note that I don't use $x = 5 \pmod{7}$ and $x = 25 \pmod{29}$, because these are are negatives of the solutions I used first, so I'll just get 149 and 54 again.

$$\begin{array}{ccc} m & 7 & 29 \\ p & 29 & 7 \\ s & 1^{-1} = 1 \pmod{7} & 7^{-1} = 25 \pmod{29} \\ a & 2 & 25 \end{array}$$

$$x = 29 \cdot 1 \cdot 2 + 7 \cdot 25 \cdot 25 = 4433 = 170 \pmod{203}.$$

Hence, $x = -170 = 33 \pmod{203}$ is another solution.

All together, the solutions are $x = 33, 54, 149, 170 \pmod{203}$. $\square$

---

34. Find a solution to $x^2 = 208 \pmod{289}$ by lifting a solution to the congruence mod 17.

Consider

$$x^2 = 208 = 4 \pmod{17}.$$

Obviously, $x = 2 \pmod{17}$ is a solution.

Method 1. Try to find a solution of the form $y = 2 + 17k$ to the original congruence:

$$\begin{aligned} y^2 &= 208 \pmod{289} \\ (2 + 17k)^2 &= 208 \pmod{289} \\ 4 + 68k + 289k^2 &= 208 \pmod{289} \\ 68k &= 204 \pmod{289} \\ 68k &= 68 \cdot 3 \pmod{289} \end{aligned}$$

I cancel the factor of 68, dividing the modulus by $(289, 68) = 17$. This gives

$$k = 3 \pmod{17}.$$

So one solution is obtained by taking $k = 3$, which gives

$$y = 2 + 17 \cdot 3 = 53 \pmod{289}.$$

Method 2. Use the algorithm given by the proof of the theorem on lifting solutions to polynomial congruences.

Let $f'(x) = x^2 - 208$, so $f'(x) = 2x$.

$$f'(2) = 4, \quad f(2) = -204.$$

Note that $17 \not| 4$.

Solve:

$$\begin{aligned} 4t &= -\frac{-204}{17} = 12 \pmod{17} \\ t &= 3 \pmod{17} \end{aligned}$$

A solution to the original congruence is given by

$$x = 2 + 17 \cdot 3 = 53 \pmod{289}.$$

The other solution is $-53 = 236 \pmod{289}$. $\square$

---

35. Suppose that p is an odd prime and $p = 19 \pmod{20}$. Compute $\left(\dfrac{-5}{p}\right)$.

First, $\left(\dfrac{-5}{p}\right) = \left(\dfrac{-1}{p}\right)\left(\dfrac{5}{p}\right)$.

Since $p = 19 \pmod{20}$, I may write $p = 19 + 20s$. Then $p = 3 \pmod{4}$, so $\left(\dfrac{-1}{p}\right) = -1$.

Similarly, $\left(\dfrac{5}{p}\right) = \left(\dfrac{p}{5}\right)$. But $p = 19 + 20s$ shows that $p = 4 \pmod{5}$, so

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

Therefore, $\left(\dfrac{-5}{p}\right) = (-1)(1) = -1$. $\square$

---

36. Compute $\left(\dfrac{180}{211}\right)$.

$$\left(\frac{180}{211}\right) = \left(\frac{5 \cdot 36}{211}\right) = \left(\frac{5}{211}\right)\left(\frac{36}{211}\right) = \left(\frac{5}{211}\right) \cdot 1 = \left(\frac{5}{211}\right).$$

Since $5 = 4 \cdot 1 + 1$,

$$\left(\frac{5}{211}\right) = \left(\frac{211}{5}\right) = \left(\frac{1}{5}\right) = 1.$$

Therefore, $\left(\dfrac{180}{211}\right) = 1$. $\square$

---

37. Compute $\left(\dfrac{375}{461}\right)$.

I'll use Jacobi symbols to simplify the computation:

$$\left(\frac{375}{461}\right) = \left(\frac{25 \cdot 15}{461}\right) = \left(\frac{15}{461}\right) = \left(\frac{461}{15}\right) = \left(\frac{11}{15}\right) =$$

$$\left(\frac{11}{3}\right)\left(\frac{11}{5}\right) = \left(\frac{2}{3}\right)\left(\frac{1}{5}\right) = (-1)(1) = -1. \quad \square$$

---

38. Convert 2781 to base 5.

5	2781	-
5	556	1
5	111	1
5	22	1
5	4	2
5	0	4

Thus, $2781 = (42111)_5$. $\square$

---

39. Express 0.26 in base 5.

a	x	bx
-	0.26	1.3
1	0.3	1.5
1	0.5	2.5
2	0.5	2.5
2	0.5	2.5

Thus, $0.26 = (0.11222\ldots)_5 = (0.11\overline{2})_5$. $\square$

---

40. Find a decimal fraction in lowest terms equal to $(0.2\overline{56})_7$.

Let $x = (0.2\overline{56})_7$. Then $49x = (25.6\overline{56})_7$, so

$$\begin{aligned} 49x &= (25.6\overline{56})_7 \\ x &= (0.2\overline{56})_7 \\ \hline 48x &= (25.4)_7 \\ 48x &= 2 \cdot 7 + 5 + 4 \cdot \frac{1}{7} \\ 48x &= \frac{137}{7} \\ x &= \frac{137}{336} \quad \square \end{aligned}$$

---

41. Express $(.1\overline{25})_6$ as a decimal fraction in lowest terms.

Let $x = (.1\overline{25})_6$. Then $36x = (12.5\overline{25})_6$, so

$$\begin{array}{rcc} 36x & = & (12.5\overline{25})_6 \\ x & = & (.1\overline{25})_6 \\ \hline 35x & = & (12.4)_6 \end{array}$$

Now

$$(12.4)_6 = 1 \cdot 6^1 + 2 \cdot 6^0 + 4 \cdot \frac{1}{6} = 8 + \frac{2}{3} = \frac{26}{3}.$$

Hence,

$$35x = \frac{26}{3}, \quad x = \frac{26}{105}. \quad \square$$

---

42. If b is an integer and $b > 1$, find a decimal fraction equal to $(0.\overline{1})_b$.

$$(0.\overline{1})_b = \frac{1}{b} + \frac{1}{b^2} + \frac{1}{b^3} + \cdots = \frac{1}{b} \cdot \sum_{n=0}^{\infty} \left(\frac{1}{b}\right)^n = \frac{1}{b} \cdot \frac{1}{1 - \dfrac{1}{b}} = \frac{1}{b-1}. \quad \square$$

43. Find the finite continued fraction expansion for $\dfrac{271}{43}$.

a	q
271	-
43	6
13	3
4	3
1	4

$$\frac{271}{43} = [6;3,3,4] = 6 + \cfrac{1}{3 + \cfrac{1}{3 + \cfrac{1}{4}}}. \quad \square$$

44. (a) Find the first 5 convergents of $[7;\overline{5,10}]$.

(b) Find the exact value of $x = [7;\overline{5,10}]$.

(a)

a_k	p_k	q_k	c_k
7	7	1	7
5	36	5	$\frac{36}{5}$
10	367	51	$\frac{367}{51}$
5	1871	260	$\frac{1871}{260}$
10	19077	2651	$\frac{19077}{2651}$

$\square$

(b)

$$x = 7 + \cfrac{1}{5 + \cfrac{1}{10 + \cfrac{1}{5 + \ddots}}}.$$

Therefore,

$$x - 7 = \cfrac{1}{5 + \cfrac{1}{10 + \cfrac{1}{5 + \ddots}}} = \cfrac{1}{5 + \cfrac{1}{10 + (x-7)}} = \cfrac{1}{5 + \cfrac{1}{x+3}} = \frac{x+3}{5x+16}.$$

Thus,

$$\begin{aligned} (5x+16)(x-7) &= x+3 \\ 5x^2 - 19x - 112 &= x+3 \\ 5x^2 - 20x - 115 &= 0 \\ x^2 - 4x - 23 &= 0 \end{aligned}$$

This gives the roots

$$x = \frac{4 \pm \sqrt{16+92}}{2} = 2 \pm 3\sqrt{3}.$$

Since x is obviously positive, it follows that $x = 2 + 3\sqrt{3}$. $\square$

---

45. Find the first 10 terms of the continued fraction expansion of $\sqrt[3]{114}$.

x_k	a_k
4.84881	4
1.17812	1
5.61409	5
1.62843	1
1.59127	1
1.69128	1
1.44659	1
2.23921	2
4.18051	4
5.53997	5
1.85197	1

$\square$

---

46. (a) Find the continued fraction expansion of $\sqrt{7}$. Find the convergents $c_0, \ldots, c_8$.

(b) Use the convergents of the continued fraction expansion of $\sqrt{7}$ to find a solution to the Fermat-Pell equation $x^2 - 7y^2 = 1$.

(a) I'll use the recursion formula

$$x_0 = x, \quad a_0 = [x_0],$$

$$x_k = \frac{1}{x_{k-1} - a_{k-1}}, \quad a_k = [x_k], \quad k \geq 1.$$

Note that since $\sqrt{7}$ is a quadratic irrational, I can stop once I see that the expansion has repeated.

x	a
$\sqrt{7}$	2
$\dfrac{1}{\sqrt{7}-2} \approx 1.54858$	1
≈ 1.82288	1
≈ 1.21525	1
≈ 4.64575	4
≈ 1.54858	1
≈ 1.82288	1

Thus, $\sqrt{7} = [2; \overline{1, 1, 1, 4}]$. The convergents are

a_k	p_k	q_k	c_k
2	2	1	2
1	3	1	3
1	5	2	$\frac{5}{2}$
1	8	3	$\frac{8}{3}$
4	37	14	$\frac{37}{14}$
1	45	17	$\frac{45}{17}$
1	82	31	$\frac{82}{31}$
1	127	48	$\frac{127}{48}$
4	590	223	$\frac{590}{223}$

Note that $\sqrt{7} \approx 2.64575$, while $\dfrac{590}{223} \approx 2.64574$. □

(b) Since the period is 4, which is even, the numerator p_3 and denominator q_3 give a solution:

$$8^2 - 7 \cdot 3^2 = 1. \quad \square$$

---

47. Find the convergents of the finite continued fraction $[1; 1, 4, 1, 4, 1, 4]$.

a_k	p_k	q_k	c_k
1	1	1	1
1	2	1	2
4	9	5	$\frac{9}{5}$
1	11	6	$\frac{11}{6}$
4	53	29	$\frac{53}{29}$
1	64	35	$\frac{64}{35}$
4	309	169	$\frac{309}{169}$

□

---

48. Find the exact value of the periodic continued fraction $[1; \overline{2, 5}]$.

Write $x = [1; \overline{2, 5}]$, so

$$x = 1 + \cfrac{1}{2 + \cfrac{1}{5 + \cfrac{1}{1 + \cfrac{1}{2 + \ddots}}}}.$$

Let $y = [\overline{2, 5}]$, so $x = 1 + \dfrac{1}{y}$. Then

$$y = 2 + \cfrac{1}{5 + \cfrac{1}{2 + \cfrac{1}{5 + \ddots}}} = 2 + \cfrac{1}{5 + \cfrac{1}{y}} = 2 + \cfrac{1}{\cfrac{5y+1}{y}} = 2 + \frac{y}{5y+1} = \frac{2(5y+1)+y}{5y+1} = \frac{11y+2}{5y+1}.$$

Clear the fraction to obtain a quadratic:

$$5y^2 + y = 11y + 2, \quad 5y^2 - 10y - 2 = 0.$$

The solutions are

$$y = \frac{10 \pm \sqrt{140}}{10}.$$

y must be positive, so

$$y = \frac{10 + \sqrt{140}}{10} = \frac{10 + 2\sqrt{35}}{10} = \frac{5 + \sqrt{35}}{5}.$$

Hence,

$$x = 1 + \cfrac{1}{\cfrac{5+\sqrt{35}}{5}} = 1 + \frac{5}{5+\sqrt{35}} = \frac{10+\sqrt{35}}{5+\sqrt{35}} = \frac{-3+\sqrt{35}}{2}. \quad \square$$

---

49. Find the rational number $\dfrac{p}{q}$ in lowest terms with $q \le 50$ which best approximates $\dfrac{\pi}{e}$.

x	a	p	q	c	error
1.15573	1	1	1	1	0.015573
6.42148	6	7	6	$\frac{7}{6}$	0.01094
2.37259	2	15	13	$\frac{15}{13}$	0.00188
2.68389	2	37	32	$\frac{37}{32}$	0.00052
1.46223	1	52	45	$\frac{52}{45}$	0.00017
2.16342	2	141	122	$\frac{141}{122}$	0.00001

I computed the first six convergents for the continued fraction expansion for $\dfrac{\pi}{e}$. I conjecture that $\dfrac{52}{45}$ is the best rational approximation with denominator less than or equal to 50.

Suppose that $\dfrac{p}{q}$ is a better approximation, and $q \le 50$. Then

$$\left|\frac{\pi}{e} - \frac{p}{q}\right| < \left|\frac{\pi}{e} - \frac{52}{45}\right| \approx 0.00017.$$

Now $q \le 50$, so

$$\frac{1}{2q^2} \ge \frac{1}{5000} = 0.0002.$$

Hence,

$$\frac{1}{2q^2} > \left|\frac{\pi}{e} - \frac{p}{q}\right|.$$

Therefore, $\frac{p}{q}$ must be a convergent. However, the table shows that no convergent with denominator less than or equal to 50 approximates $\frac{\pi}{e}$ better than $\frac{52}{45}$. Hence, there is no such $\frac{p}{q}$, and $\frac{52}{45}$ is the best rational approximation with denominator less than or equal to 50. $\square$

The best thing for being sad is to learn something. - MERLYN, in T.H. WHITE'S *The Once and Future King*