Algebra and Number Theory Solutions

1. Let a_1, a_2, …, a_n be a geometric progression with $a_1 = \sqrt{2}$ and $a_2 = \sqrt[3]{3}$. What is
$$\frac{a_1 + a_{2013}}{a_7 + a_{2019}}?$$

   Proposed by Xiao Liu

   Answer: $\frac{8}{9}$

   Solution. Let $r = \frac{a_2}{a_1} = \frac{\sqrt[3]{3}}{\sqrt{2}}$ denote the ratio between consecutive terms of the geometric progression. Then $a_7 = r^6 a_1$ and $a_{2019} = r^6 a_{2013}$, so
$$\frac{a_1 + a_{2013}}{a_7 + a_{2019}} = \frac{a_1 + a_{2013}}{r^6(a_1 + a_{2013})} = \frac{1}{r^6} = \boxed{\frac{8}{9}}.$$

2. For all positive integers n, let $f(n)$ return the smallest positive integer k for which $\frac{n}{k}$ is not an integer. For example, $f(6) = 4$ because 1, 2, and 3 all divide 6 but 4 does not. Determine the largest possible value of $f(n)$ as n ranges over the set $\{1, 2, \ldots, 3000\}$.

   Proposed by Gunmay Handa

   Solution. Note that $f(n) \geq k$ if and only if n is divisible by every integer between 1 and $k - 1$, i.e. n is divisible by $\operatorname{lcm}(1, 2, \ldots, k - 1)$. Now notice that
$$\operatorname{lcm}(1, 2, \ldots, 10) = 2520 \qquad \text{but} \qquad \operatorname{lcm}(1, 2, \ldots, 10, 11) = 27720.$$
   Thus $N = 2520$ satisfies $f(N) = 11$ and no integer $n \leq 3000$ can have $f(n) \geq 12$, meaning the answer is $\boxed{11}$

3. Let $P(x)$ be a quadratic polynomial with real coefficients such that $P(3) = 7$ and
$$P(x) = P(0) + P(1)x + P(2)x^2$$
   for all real x. What is $P(-1)$?

   Proposed by David Altizio

   Answer: $\frac{7}{5}$

   Solution. Plugging $x = 1$ and $x = 2$ into the given equality yields the system of equations
$$P(1) = P(0) + P(1) + P(2) \qquad \text{and} \qquad P(2) = P(0) + 2P(1) + 4P(2).$$
   The first equality simplifies to $P(0) = -P(2)$, and plugging this into the second equation yields $P(1) = -P(2)$. Thus $P(x) = t(x^2 - x - 1)$ for some $t \in \mathbb{R}$. Now plugging in $x = 3$ yields $t = \frac{7}{5}$, and so $P(-1) = \boxed{\frac{7}{5}}$.

   Remark. One can actually construct for any n a family of polynomials P such that
$$P(x) = P(0) + P(1)x + \cdots + P(n)x^n$$
   for every x. This is because by plugging in $k = 0, 1, \ldots, n$ we obtain that
$$P(k) = P(0) + P(1)k + \cdots + P(k)k^n$$
   for all such k. Writing this as a linear system of equations in $P(0)$, $P(1)$, …, $P(k)$ gives the system $A\vec{x} = \vec{x}$ for $\vec{x} = (P(0)\ P(1)\ \ldots\ P(n))$ and
$$A = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 \\ 1 & 1 & 1 & \cdots & 1 \\ 1 & 2 & 4 & \cdots & 2^n \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & n & n^2 & \cdots & n^n \end{bmatrix}.$$

It is trivial to see that $A - I$ has rank at most $n-1$ (due to the top row consisting of only zeroes), and so this system has a one-parameter family of solutions. Constructing the resulting polynomial from the values of $P(0), \ldots, P(n)$ can be done through Lagrange Interpolation.

4. Determine the sum of all positive integers n between 1 and 100 inclusive such that

$$\gcd(n, 2^n - 1) = 3.$$

Proposed by David Altizio

Answer: 360

Solution. First note that if n is such a positive integer, then $3 \mid n$ and $3 \mid 2^n - 1$. The former statement implies n is divisible by 3, while the latter statement implies that $2^n \equiv 1 \pmod 3 \Leftrightarrow 2 \mid n$. Thus $n = 6k$ for some positive integer $1 \le k \le 16$. Note that it is impossible for $\gcd(n, 2^n - 1)$ to be even, so it remains to show that the k does not introduce any new factors into the greatest common divisor. We now case.

- First note that $k = 1$ yields $\gcd(6, 2^6 - 1) = \gcd(6, 63) = 3$, so $n = 6$ works.
- Now suppose $k = p^\ell$ for some prime p. Note that by Fermat's Little Theorem, $2^p \equiv 2 \pmod p$, so in particular
$$2^{p^\ell} \equiv (2^p)^{p^{\ell-1}} \equiv 2^{p^{\ell-1}} \equiv \cdots \equiv 2 \pmod p.$$
Thus $2^n - 1 \equiv 2^6 - 1 \equiv 63 \pmod p$; this forces $p \notin \{3, 7\}$. As a result, we obtain seven new values of n, namely $n = 6k$ for $k \in \{2, 4, 5, 8, 11, 13, 16\}$. Note also that from this analysis we obtain that k cannot be divisible by 3 or 7.
- Surprisingly, this leaves only $k = 10$ left. But this fails too, as $2^{60} - 1$ is divisible by $2^4 - 1 = 15$, and so 5 divides the greatest common divisor.

We thus have 8 integers total whose sum is $\boxed{360}$.

5. Let x_n be the smallest positive integer such that 7^n divides $x_n^2 - 2$. Find $x_1 + x_2 + x_3$.

Proposed by Cody Johnson

Answer: 121

Solution. First remark that $x_1^2 \equiv 2 \pmod 7$ implies $x_1 \equiv 3, 4 \pmod 7$, so $x_1 = 3$.

Now to compute x_2, note that $x^2 \equiv 2 \pmod{49}$ certainly implies $x^2 \equiv 2 \pmod 7$, so at the very least $x \equiv 3, 4 \pmod 7$. Let $x = 7y + r$, where $y \in \{0, 1, \ldots, 6\}$ and $r \in \{3, 4\}$. Then

$$2 \equiv x_n^2 \equiv (7y + r)^2 \equiv 14yr + r^2 \pmod{49}.$$

In the $r = 3$ case this simplifies to $42y \equiv -7 \pmod{49}$, so $y \equiv 1 \pmod 7$. The $r = 4$ case is analogous and leads to $y \equiv 5 \pmod 7$. It follows that the solutions to $x^2 \equiv 2 \pmod{49}$ are $x \equiv \pm 10 \pmod{49}$, so $x_2 = 10$.

In a similar fashion, note that $x^2 \equiv 2 \pmod{7^3}$ certainly implies $x \equiv \pm 10 \pmod{49}$. Thus we may let $x = 49y + r$ for $r \in \{10, 39\}$ and $y \in \{0, 1, 2, 3, 4, 5, 6\}$, which implies

$$2 \equiv x_n^2 \equiv (49y + r)^2 \equiv 98yr + r^2 \pmod{7^3}.$$

Solving this similarly yields $(r, y) = (10, 2)$ and $(r, y) = (39, 4)$; thus the solutions to $x^2 \equiv 2 \pmod{7^3}$ are $x \equiv \pm 108 \pmod{7^3}$, so $x_3 = 108$.

All in all, $x_1 + x_2 + x_3 = 3 + 10 + 108 = \boxed{121}$.

Remark. This technique can be used to prove that $x^2 \equiv 2 \pmod{7^n}$ has a solution for all positive integers n.

6. Let a, b and c be the distinct solutions to the equation $x^3 - 2x^2 + 3x - 4 = 0$. Find the value of

$$\frac{1}{a(b^2+c^2-a^2)} + \frac{1}{b(c^2+a^2-b^2)} + \frac{1}{c(a^2+b^2-c^2)}.$$

Proposed by Gunmay Handa

Answer: $\frac{1}{8}$

Solution. Note that

$$a^2+b^2+c^2 = (a+b+c)^2 - 2(ab+bc+ca) = 2^2 - 2\cdot 3 = -2.$$

Thus

$$\frac{1}{a(b^2+c^2-a^2)} = \frac{1}{a(-2-2a^2)} = \frac{-1}{2a(1+a^2)}.$$

However, observe that

$$\frac{-1}{2a(1+a^2)} = \frac{-1}{2a+2(2a^2-3a+4)} = \frac{-1}{4(a^2-a+2)} = \frac{-(a-1)}{4(a^2-a+2)(a-1)} = \frac{1-a}{8}$$

whence the desired answer is simply

$$\frac{1-a}{8} + \frac{1-b}{8} + \frac{1-c}{8} = \frac{3-a-b-c}{8} = \boxed{\frac{1}{8}}.$$

OR

Solution. As above, we have

$$\frac{1}{a(b^2+c^2-a^2)} = \frac{1}{a(-2-2a^2)} = \frac{-1}{2a(1+a^2)} = \frac{1}{4}\left[\frac{1}{a+i} - \frac{1}{a-i}\right] - \frac{1}{2a}.$$

It follows that, upon letting $F(r) = \frac{1}{r-a} + \frac{1}{r-b} + \frac{1}{r-c}$, it suffices to compute $\frac{1}{2}F(0) - \frac{1}{4}(F(i)+F(-i))$. We now claim that

$$F(r) = \frac{3r^2-4r+3}{r^3-2r^2+3r-4} \qquad \text{for all } r \notin \{a,b,c\}.$$

There are several ways to prove this fact, but perhaps the most elementary is through direct expansion, as one may write

$$\begin{aligned}\frac{1}{a-r} + \frac{1}{b-r} + \frac{1}{c-r} &= \frac{(a-r)(b-r)+(b-r)(c-r)+(c-r)(a-r)}{(a-r)(b-r)(c-r)} \\ &= \frac{ab+bc+ca-2r(a+b+c)+3r^2}{(a-r)(b-r)(c-r)} = \frac{3r^2-4r+3}{r^3-2r^2+3r-4}.\end{aligned}$$

It is now a work of computation to derive the answer of $\boxed{\frac{1}{8}}$.

Remark. The astute reader may recognize that $F(r) = \frac{P'(r)}{P(r)}$, where $P(x) = x^3 - 2x^2 + 3x - 4$. This is no coincidence, and it is an instructive exercise in one-dimensional calculus to prove this using the Product Rule.

7. For all positive integers n, let

$$f(n) = \sum_{k=1}^{n} \varphi(k) \left\lfloor \frac{n}{k} \right\rfloor^2.$$

Compute $f(2019) - f(2018)$.

Proposed by David Altizio

Answer: 11431

Solution. The crucial claim is that

$$f(n) = \sum_{(s,t)\in[n]^2} \gcd(s,t).$$

To prove this, for each integer k let

$$S_k = \{(i,j) \in [n]^2 \mid \text{both } i \text{ and } j \text{ are divisible by } k\}.$$

It is easy to see that $|S_k| = \lfloor \frac{n}{k} \rfloor^2$, so

$$\sum_{k=1}^{n} \varphi(k) \left\lfloor \frac{n}{k} \right\rfloor^2 = \sum_{k=1}^{n} \sum_{(s,t)\in[n]^2} \varphi(k)\mathbf{1}_{S_k}(s,t) = \sum_{(s,t)\in[n]^2} \sum_{k=1}^{n} \varphi(k)\mathbf{1}_{S_k}(s,t).$$

For fixed $(s,t) \in [n]^2$, the inner sum runs over all k for which $k \mid s$ and $k \mid t$ simultaneously, i.e. $k \mid \gcd(s,t)$. Thus in fact the sum equals

$$\sum_{(s,t)\in[n]^2} \sum_{d\mid\gcd(s,t)} \varphi(k) = \sum_{(s,t)\in[n]^2} \gcd(s,t)$$

as desired, where in the last step we use the well-known equality $\sum_{d\mid n} \varphi(d) = n$. In turn, $f(2019) - f(2018)$ only sums over all pairs (i,j) for which either $i = 2019$ or $j = 2019$, which means the desired sum is $2\sum_{j=1}^{2019} \gcd(j, 2019) - 2019$.

One can evaluate this sum using a bit of convolution trickery (see the discussion for **2015 Putnam A3** for more information), but it is also not bad to compute explicitly. Specifically, note that $2019 = 3 \cdot 673$, so the summand is either 1, 3, 673, or 2019. It takes these values precisely $\varphi(2019) = 1344$, 672, 2, and 1 times respectively, and so

$$\sum_{j=1}^{2019} \gcd(j, 2019) = 1 \cdot 1344 + 3 \cdot 672 + 673 \cdot 2 + 2019 = 6725.$$

It follows that the desired answer is $2 \cdot 6725 - 2019 = \boxed{11431}$.

8. It is given that the roots of the polynomial $P(z) = z^{2019} - 1$ can be written in the form $z_k = x_k + iy_k$ for $1 \le k \le 2019$. Let Q denote the monic polynomial with roots equal to $2x_k + iy_k$ for $1 \le k \le 2019$. Compute $Q(-2)$.

Proposed by David Altizio

Answer: $-\dfrac{1+3^{2019}}{2^{2018}}$

Solution. Recall that for all k we have $x_k = \frac{z_k+\overline{z_k}}{2}$ and $iy_k = \frac{z_k-\overline{z_k}}{2}$, so

$$2x_k + iy_k = \frac{3z_k + \overline{z_k}}{2} = \frac{3z_k^2+1}{2z_k}.$$

Thus

$$Q(-2) = \prod_{k=1}^{2019} \left(-2 - \frac{3z_k^2+1}{2z_k}\right) = \frac{(-1)^{2019}}{2^{2019}} \prod_{k=1}^{2019} \frac{3z_k^2+4z_k+1}{z_k}$$
$$= -\frac{1}{2^{2019}} \prod_{k=1}^{2019} (3z_k+1)(z_k+1) = -\frac{3^{2019}}{2^{2019}} P(-\tfrac{1}{3})P(-1) = \boxed{-\frac{1+3^{2019}}{2^{2018}}}.$$

9. Let $a_0 = 29$, $b_0 = 1$ and
$$a_{n+1} = a_n + a_{n-1} \cdot b_n^{2019}, \qquad b_{n+1} = b_n b_{n-1}$$
for $n \geq 1$. Determine the smallest positive integer k for which 29 divides $\gcd(a_k, b_k - 1)$ whenever a_1, b_1 are positive integers and 29 does not divide b_1.

Proposed by Vijay Srinivasan

Answer: 168

Solution. Note that the first equation simplifies modulo 29 to
$$a_{n+1} \equiv a_n + a_{n-1} \cdot b_n^3 \pmod{29}.$$
Upon making the shift $b_n \mapsto b_n^3$ (which doesn't break the problem statement as the map $x \mapsto x^3$ is injective modulo 29), the second recurrence is preserved, so we will instead work with the recurrence relation
$$a_{n+1} \equiv a_n + a_{n-1} \cdot b_n \pmod{29}.$$
Now $b_0 = 1$ combined with an induction argument yields $b_n = c^{F_n}$ for $c = b_1$. As a result, the first equation rewrites as
$$a_{n+1} \equiv a_n + a_{n-1} c^{F_n} \pmod{29}.$$
If $a_1 \equiv 0 \pmod{29}$, then all terms of the sequence are divisible by 29. Otherwise, we can assume $a_1 = 1$ by homogeneity. We now claim that
$$a_n = \sum_{k<F_n} c^k = \frac{c^{F_n} - 1}{c - 1}.$$
To prove this, we use strong induction on n. The base cases of $n = 0$ and $n = 1$ are easy. Now for the inductive step, assume the result holds for all $k \leq n$. Then by the inductive hypothesis,
$$a_{n+1} \equiv a_n + a_{n-1} c^{F_n} \equiv \sum_{k<F_n} c^k + c^{F_n} \sum_{k<F_{n-1}} c^k \overset{(*)}{\equiv} \sum_{k<F_n} c^k + \sum_{F_n \leq k < F_{n+1}} c^k \equiv \sum_{k<F_{n+1}} c^k \pmod{29},$$
where in $(*)$ we crucially use the fact that every positive integer has a unique Zeckendorf representation.

We now split into cases.

- If $c \neq 1 \pmod{29}$, it suffices to have $c^{F_n} \equiv 1 \pmod{29}$. By taking c to be a primitive root mod 29 ($c = 2$, for instance), this is equivalent to $28 \mid F_n$, implying n is divisible by $\operatorname{lcm}(6, 8) = 24$.
- If $c = 1$, then the sum is congruent to F_n modulo 29, and so it suffices to find the smallest n for which $29 \mid F_n$. This after some computation is 14.

Combining our two cases shows that the answer is $\operatorname{lcm}(14, 24) = \boxed{168}$.

10. Determine the number of positive integers $2 \leq n \leq 50$ such that all coefficients of the polynomial
$$\left(x^{\varphi(n)} - 1\right) - \prod_{\substack{1 \leq k \leq n \\ \gcd(k,n)=1}} (x - k)$$
are divisible by n.

Proposed by Manuel Fernandez

Answer: 19

Solution. The crucial claim is that if $n \neq 4$, then n is either prime or twice a Fermat prime.

Note that the result holds for $n = 2$, and $n = 4$, so assume $n \notin \{2, 4\}$. First note that by looking at the constant term of this polynomial, we must have

$$\prod_{\substack{1\le k\le n\\ \gcd(k,n)=1}} k \equiv -1 \pmod{n},$$

where in particular we use the fact that $\varphi(n)$ is even. By **HMMT 2016 Algebra #8**, this means n is either p^k, or $2p^k$ for some odd prime p and some integer $k \ge 1$; in particular, there must exist a primitive root modulo n.

In the $n = p^k$ case, assume $k \ge 2$. Then consider the power sums

$$S_\ell := \sum_{\substack{1\le j\le n\\ \gcd(j,n)=1}} j^\ell$$

modulo p^k. Note that $S_\ell \equiv 0 \pmod{n}$ for $1 \le \ell \le p-2$: if g is a generator of the multiplicative group $(\mathbb{Z}/p^k\mathbb{Z})^*$, then

$$S_\ell \equiv \sum_{j=0}^{\varphi(p^k)-1} g^{\ell j} \equiv \frac{g^{\ell\varphi(p^k)}-1}{g^\ell - 1} \equiv 0 \pmod{p^k}.$$

However, S_{p-1} is not zero; the following lemma is crucial to proving this claim.

Lemma 1. *For all positive integers k,*

$$\sum_{j=1}^{p^k} j^{p-1} \equiv (p-1)p^{k-1} \pmod{p^k}.$$

Proof. The following proof of this lemma is based on **alifenix-**'s solution to **USA December EGMO TST 2019 #3** on the Art of Problem Solving fora. We proceed by induction on k. For $k = 1$ the result follows by Fermat's Little Theorem. For the inductive step, write

$$\sum_{j=1}^{p^{k+1}} j^{p-1} = \sum_{i=0}^{p-1}\sum_{j=1}^{p^k} (ip^k + j)^{p-1}.$$

The crucial fact we need is that the inner sum is constant modulo p^k (i.e. it doesn't change as i changes). Indeed,

$$\sum_{j=1}^{p^k} (ip^k + j)^{p-1} \equiv \sum_{j=1}^{p^k} \left(j^{p-1} + i(p-1)p^k j^{p-2}\right) \pmod{p^k};$$

the left sum is equal to $p^{k-1}(p-1)$ by our IH, while the right term is zero due to the above primitive root argument. Hence

$$\sum_{j=1}^{p^{k+1}} j^{p-1} \equiv p \cdot p^{k-1}(p-1) \equiv p^k(p-1) \pmod{p^{k+1}},$$

and so we are done. □

As a result,

$$S_{p-1} = \sum_{j=1}^{p^k} j^{p-1} - p^{p-1}\sum_{j=1}^{p^{k-1}} j^{p-1} \equiv p^{p-1}(p-1) \not\equiv 0 \pmod{p^k},$$

where in the last step we use the IH on both terms and the fact that $p-1 \ge 2$. Thus the coefficient of x^{p-1} is nonzero modulo p^k, and so $k > 1$ gives a contradiction. We must have $k = 1$, and in that case the statement is well-known to be true.

Now we proceed with the $2p^k$ case. By Chinese Remainder Theorem, the congruence in the problem statement must hold modulo 2. But in this case the product collapses to

$$\prod_{\substack{1\le k\le n\\ \gcd(k,n)=1}} (x-k) \equiv \prod_{\substack{1\le k\le n\\ \gcd(k,n)=1}} (x-1) \equiv (x-1)^{\varphi(2p^k)} \pmod 2.$$

Now write $\varphi(2p^k) = s\cdot 2^t$ where s is odd. Then

$$(x-1)^{\varphi(2p^k)} \equiv \left[(x-1)^{2^t}\right]^s \equiv (x^{2^t}-1)^s \pmod 2.$$

This cannot equal $x^{\varphi(n)}-1$ modulo 2 unless $s=1$, i.e. $p^{k-1}(p-1)$ has no odd factors. It follows that $k=1$ and $p-1=2^\ell$, meaning that n is twice a Fermat prime. It remains to show that such a p works; but this follows from the fact that n is even iff $n+p$ is odd, and so modulo p this reduces to the previous case.

Finally, within the range $[1,50]$, there are 15 prime numbers and three integers which are twice a Fermat prime (6, 10, and 34). Remembering to add the 4 back in, it follows that the desired count is $\boxed{19}$.