Solutions to Problem Set 5: Number Theory

From the Eötvös Competitions (Hungarian high school competitions)

1894.1 Prove that the expressions $2x + 3y$ and $9x + 5y$ are divisible by 17 for the same set of integral values of x and y. [Can you find a generalization?]

Observe that $13(2x+3y) = 9x+5y$ and $2x+3y = 4(9x+5y)$ modulo 17. Therefore, because both 4 and 13 are relatively prime to 17, each linear combination is zero modulo 17 if and only if the other one is.

In general, suppose $ad - bc$ is a prime p. Expressions $ax + by$ and $cx + dy$ are simultaneously divisible by p if and only if the vectors (a, b) and (c, d) are linearly dependent in the field of p elements, as we know from linear algebra. This means there exists a nonzero m such that $(c, d) = m(a, b)$, a value easily found by solving either of the equations $c = ma$ or $d = mb$ modulo p.

1896.1 Prove that $\log(n) = k \log(2)$, where n is any whole number and k is the number of distinct primes dividing n.

Use the Fundamental Theorem of Arithmetic to write $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ for distinct primes p_1, …, p_k. Then $\log(n) = e_1\log(p_1) + \ldots + e_k\log(p_k) = \log(2) + \ldots + \log(2) = k\log(2)$ because each of the $e_i = 1$ and each of the $p_i = 2$.

1898.1 Determine all positive integers n for which $2^n + 1$ is divisible by 3.

Working modulo 3 gives $2^n + 1 = 0$. But the powers of 2 mod 3 are successively -1, 1, -1, etc., showing immediately that n must be a positive odd integer.

1899.3 Prove that, for any natural number n, the expression $2903^n - 803^n - 464^n + 261^n$ is divisible by 1897.

Use the fact that $x^n - y^n$ is divisible by $(x - y)$ to deduce (a.1) $2903^n - 803^n$ is divisible by $2903 - 803 = 2100$; (a.2) $-464^n + 261^n$ is divisible by $261 - 464 = -203$; (b.1) $2903^n - 464^n$ is divisible by $2903 - 464 = 2439$; and (b.2) $-803^n + 261^n$ is divisible by $261 - 803 = 342$. Combining (a.1) and (a.2) shows the expression is divisible by gcd(2100, -203) = 7 while combining (b.1) and (b.2) shows the expression is divisible by gcd(2439, 342) = 271. Since 7 and 271 are relatively prime, we may conclude the expression is divisible by 7*271 = 1897.

1900.1 Let a, b, c, d be fixed integers with d not divisible by 5. Assume that m is an integer for which $am^3 + bm^2 + cm + d$ is divisible by 5. Prove there exists an integer n for which $dn^3 + cn^2 + bn + a$ is also divisible by 5.

m is not divisible by 5, for otherwise $am^3 + bm^2 + cm + d$ would be divisible by 5, contrary to the assumption. Therefore m has a multiplicative inverse n modulo 5. Working modulo 5 gives $0 = n^3(0) = n^3(am^3 + bm^2 + cm + d) = a(nm)^3 + bn(nm)^2 + cn^2(nm) + dn^3 = dn^3 + cn^2 + bn + a$, QED.

1901.1 Prove that, for any positive integer n, $1^n + 2^n + 3^n + 4^n$ is divisible by 5 if and only if n is not divisible by 4.

If n is divisible by 4, write $n = 4k$ for some integer k. Fermat's Theorem asserts $a^4 = 1$ modulo 5 for all integers a. Therefore $a^n = a^{4k} = (a^4)^k = 1^k = 1$ for all a. In particular, $1^n + 2^n + 3^n + 4^n = 1 + 1 + 1 + 1 = 4 \neq 0 \bmod 5$.

In the other direction, suppose n is not divisible by 4. Write $4 = 2^2$ and $3 = 2^3$ modulo 5. Then $1^n + 2^n + 3^n + 4^n = 2^{4n} + 2^n + 2^{3n} + 2^{2n} = 1 + (2^n)^1 + (2^n)^2 + (2^n)^3$. Multiplying this by $2^n - 1$ (which is not zero) gives $(2^n)^4 - 1$, which is zero. This can happen only if $1^n + 2^n + 3^n + 4^n = 0$, QED.

1901.2 Let a and b be two natural numbers whose greatest common divisor is d. Prove that exactly d of the numbers a, $2a$, $3a$, …, $(b\text{-}1)a$, ba are divisible by b.

Because a is a multiple of d, write $a = kd$ for some integer k. Working modulo b, the numbers are kd, $2kd$, …, $(b\text{-}1)kd$, and 0. However, since d is the gcd of a and b, k must be relatively prime to b. Therefore we can multiply all of these b integers by the multiplicative inverse of k to get d, $2d$, …, $(b\text{-}1)d$, and 0, without changing the number of zeros. The only ones of these equal to zero modulo b are the multiples b/d, $2b/d$, …, $(d\text{-}1)b/d$, and 0, of which there are exactly d.

1903.1 Let $n = 2^{p-1}(2^p - 1)$ and suppose $2^p - 1$ is prime. Prove that the sum of all (positive) divisors of n, not including n itself, is exactly n.

We are given the prime factorization of n. Its divisors consist of all the numbers 2^q and $2^q(2^p\text{-}1)$ with $0 \le q \le p\text{-}1$. Their sum therefore is $(1 + 2 + \ldots + 2^{p-1})(1 + 2^p - 1) = 2^p(2^p - 1) = n + n$. Subtracting off n—since we included n itself in the sum of divisors—yields n, QED.

1905.1 For given positive integers n and p, find necessary and sufficient conditions for the system of equations $x + py = n$, $x + y = p^z$ to have a solution (x, y, z) of positive integers. Prove also that there is at most one such solution.

This is a set of two linear equations in the two unknowns x and y. The determinant is $1\text{-}p$. Consider then two cases, depending on whether the determinant is zero or not. If it's zero, then $p = 1$ and the second equation is $x + y = 1$, which admits no positive solutions in x and y. Therefore the determinant must be nonzero, leading to a unique (real) solution $x = (n\text{-}p^{z+1})/(1\text{-}p)$ and $y = (p^z\text{-}n)/(1\text{-}p)$. If they are both to be positive, then since $1\text{-}p$ is negative, we need $n < p^{z+1}$ and $p^z < n$.

In summary, then, p must be 2 or larger and n must lie strictly between two successive powers of p, differing from each of them by a multiple of $p\text{-}1$. In such cases the value of z is determined uniquely as the smallest power of p less than n and x and y are determined uniquely as solutions of a nondegenerate system of linear equations.

Putnam Problems

1940.1: Prove that if $f(x)$ is a polynomial with integral coefficients, and there exists an integer k such that none of the integers $f(1), f(2), \ldots, f(k)$ is divisible by k, then $f(x)$ has no integral root.

If f has an integral root a, then—working modulo k—$f(a)$ is still zero. But, modulo k, a is one of the integers 1, 2, …, k. This proves the contrapositive, QED.

1957.B1: Consider the determinant $|a_{ij}|$ of order 100 with $a_{ij} = i \times j$. Prove that if the absolute value of each of the 100! terms in the expansion of this determinant is divided by 101 then the remainder in each case is 1.

By definition, any term is a product of $i * \mathbf{s}(i)$ for some permutation $\mathbf{s}$ as i ranges from 1 to 100. Therefore the term equals 100! * 100!, which by Wilson's Theorem (and the fact 101 is prime) is congruent to (-1)*(-1) = 1 modulo 101, QED.

1958.B2: Prove that the product of four consecutive positive integers is never a perfect square or cube.

For some integer $n > 0$, write the product as $n(n+1)(n+2)(n+3) = (n^2+3n+2)(n^2+3n) = (n^2+3n+1)^2 - 1$. If this is to equal a square a^2, then $(n^2+3n+1+a)(n^2+3n+1-a) = (n^2+3n+1)^2 - a^2 = 1$, showing that $n^2+3n+1+a$ is a factor of 1. We may assume $a > 0$ and, since $n > 0$, $n^2+3n+1+a > 5$, which cannot be a factor of 1: a contradiction. Therefore the product of four consecutive integers is never a perfect square.

The trick for the second part is to observe that one of the four numbers n, …, $n+3$ must be relatively prime to the other three. This lets us compare a product of *three* numbers to a cube. The trick is accomplished by looking at the middle two values, $n+1$ and $n+2$. Each is relatively prime to its immediate neighbors. Whichever one is odd is also relatively prime to all three. This gives two cases:

$n+1$ is odd: In this case, both $n+1$ and $n(n+2)(n+3) = n^3 + 5n^2 + 6n = (n+1)^3 + 2n^2 + 3n - 1$ must be cubes. The latter, however, lies strictly between the two successive cubes $(n+1)^3$ and $(n+2)^3 = (n+1)^3 + 3n^2 + 9n + 7$, a contradiction.

n is odd: Now, both n and $(n+1)(n+2)(n+3) = n^3 + 6n^2 + 11n + 6 = (n+1)^3 + 3n^2 + 8n + 5$ must be cubes. The latter also lies between two successive cubes, again a contradiction.

Having ruled out all possible cases, we conclude the product of four consecutive positive integers is never a perfect cube.

By the way, if the product of four consecutive integers were a cube, then $(n^2+3n+1)^2 - 1 = a^3$ for some positive a. Setting $b = n^2+3n+1$ would give an integral solution to $b^2 - 1 = a^3$ with $b > 4$. Indeed, the only solutions to this equation are $(a, b) = (0, -1), (\pm 1, 0)$, and $(\pm 3, 2)$.

1960.B4: Consider the arithmetic progression a, $a + d$, $a + 2d$, …, where a and d are positive integers. For any positive integer k, prove that the progression has either no exact k^{th} powers or infinitely many.

Suppose the progression has an exact k^{th} power, say $b^k = a + md$ for some nonnegative m. Then the Binomial Theorem shows $(b+d)^k = b^k + d$(sum of positive integers) $= a + md +$ sum of positive integers $= a + nd$ for a positive integer n strictly greater than m. Therefore the progression must have infinitely many exact k^{th} powers, because this calculation shows it cannot have a largest k^{th} power, QED.

1963.B2: Let S be the set of all numbers of the form 2^m3^n, where m and n are integers, and let P be the set of all positive real numbers. Is S dense in P?

Equivalently, taking logarithms to the base 2, we may ask whether the numbers of the form $m + n\lg(3)$ are dense in the set of all Real numbers, because the logarithm is continuous and one-to-one. Apply the Euclidean Algorithm to the numbers 1 and lg(3): $\lg(3) = 1 + a_1$; $1 = k_2a_1 + a_2$, etc., with $|a_{i+1}| \le |a_i|/2$ in every case (by allowing negative remainders and choosing a remainder of the smallest possible absolute value at each step). By induction on i, beginning with $a_1 < ½$, we conclude that $|a_i| < 2^{-i}$ for all i. If the algorithm does not terminate, we can thereby express integral multiples of *arbitrarily small* positive Real numbers as integral linear combinations of 1 and lg(3), proving that these are dense. But the algorithm cannot terminate, for otherwise then lg(3) would be rational, implying some nontrivial integral power of 3 equals an integral power of 2, which is impossible because 2 and 3 are relatively prime. QED.

Additional Problems

1. (Donald Knuth, *The Art of Computer Programming,* Volume 2, exercise 4.3.2#13, *Automorphic numbers*). "An n-digit decimal number $x > 1$ is called an "automorph" by recreational mathematicians if the last n digits of x^2 are equal to x. For example, 9376 is a 4-digit automorph, since $9376^2 = 87909376$. [See *Scientific American* **218** (January 1968), 125.]

   (a) Prove that an n-digit number $x > 1$ is an automorph if and only if $x \bmod 5^n = 0$ or 1 and $x \bmod 2^n = 1$ or 0, respectively.

Working modulo 10^n we require $x^2 - x = 0$. Clearly this must also be true modulo 5^n and 2^n simultaneously, where the polynomial factors as $x(x-1)$, with unique roots 0 and 1. Conversely, if x is a solution of $x^2 - x = 0$ modulo 5^n and 2^n, then it is a solution modulo 10^n by the Chinese Remainder Theorem (using the fact that 5^n and 2^n are relatively prime).

   (b) Prove that if x is an n-digit automorph, then $(3x^2 - 2x^3) \bmod 10^{2n}$ is a $2n$-digit automorph.

The notation (a, b) represents the number $a10^n + b$ modulo 10^{2n}. Write $x = (z, y)$. Because x is an n-digit automorph, we know $x^2 = (2zy, y^2) = (w, y)$ for some w, whence $(0, y^2) = (w-2zy, y)$. Observe that $(y^2, 0) = (y, 0)$. Therefore $3x^2 = (3w, 3y)$ and $2x^3 = 2(z, y)*(w, y) = (2[z+w]y, y^2) = (w+wy-zy, y)$. Thus $(3x^2 - 2x^3) = (w-2wy+2zy, y)$. Squaring this yields the same

thing by virtue of the observation: $(w\text{-}2wy+2zy, y)*(w\text{-}2wy+2zy, y) = (2y(w\text{-}2wy+2zy), y^2) = (2wy\text{-}4wy^2+4zy^2+w\text{-}2zy, y) = (w\text{-}2wy+2zy, y)$. Therefore $(3x^2 - 2x^3)$ is a $2n$-digit automorph.

(c) Given that $cx = 1$ (modulo y), find a simple formula for a number c' depending on c and x but not on y, such that $c'x^2 = 1$ (modulo y^2)."

2. (Knuth, exercise 4.4#4.) "(a) Prove that every real number with a terminating *binary* representation also has a terminating *decimal* representation. (b) Find a simple condition on the positive integers b and B that is satisfied if and only if every real number that has a terminating radix-b representation also has a terminating radix-B representation."

(a) is a special case of (b), so we prove (b). The condition is that b must divide some power N of B. This is seen by considering how to represent $1/b$ in base B. Let this representation be $1/b = \sum_{i=1}^{N} a_i B^{-i}$. Multiplying both sides by bB^N gives $B^N = b\sum_{i=1}^{N} a_i B^{N-i}$, showing that b divides B^N, since the sum is now an integer. This condition is in fact sufficient because if b divides B^N, we can work backwards to expand B^N/b in nonnegative powers of B, then divide by bB^N to express $1/b$ as a terminating base-B representation of length at most N. Accordingly, $1/b^2$ has a terminating representation of length at most N, as is seen by multiplying out the product and performing any necessary carries. By induction (repeatedly multiply the expression for $1/b$) the base-B representation of b^{-j} terminates within jN digits for all $j > 0$. Since any real number with a terminating base-b representation is an integral linear combination of finitely many b^{-j}, we can now use these expansions of the b^{-j} to obtain a representation as a finite integral linear combination of the B^{-j}. All that remains is to perform the usual carrying algorithm to reduce each of the coefficients to the range 0, …, B-1.

For example, every terminating base-4 representation has a terminating decimal representation, because 4 divides 10^2. However, some decimal representations, such as $1/5 = 0.2$, have no terminating base-4 representation, because 10 divides no power of 4.

As an example of the procedure given in the proof, consider the terminating base-4 expression 0.13. We write $¼ = 0.25$ and $¼^2 = 0.0625$ in base 10. Then, 0.13 base 4 = 1*¼ + 3*¼^2 = 1*0.25 + 3*0.0625 in base 10 = 2*0.1 + 1*0.01 + 3*0.06 + 3*0.002 + 3*0.0005 = 2*0.1 + 19*0.01 + 6*0.001 + 15*0.0001 = 0.4375. The carries took place in the last step.

Another way to state the result is that every prime dividing b must also divide B.

3. (Knuth, exercise 4.5.2#3.) "Show that the number of ordered pairs of positive integers (u, v)" such that the least common multiple of u and v is n equals the number of divisors of n^2.

Write $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ as a product of distinct prime powers. Let $[f_1, f_2, \ldots, f_k]$ denote the product $p_1^{f_1} p_2^{f_2} \cdots p_k^{f_k}$. Then u must equal $[u_1, u_2, \ldots, u_k]$ and v equal $[v_1, v_2, \ldots, v_k]$ with all components between 0 and the corresponding e. Moreover, the maximum of u_i and v_i must equal e_i for each i. Associate each such pair (u, v) with the integer $e - u$ if $u < e$ or with $e + v$ otherwise. This is a bijection whose inverse associates the value g with $(e\text{-}g, e)$ when $g < e$ and

with $(e, g\text{-}e)$ otherwise. Thus the set of ordered pairs in question is in one-to-one correspondence with all $[g_1, g_2, \ldots, g_k]$ whose coordinates lie between 0 and $2e_i$, inclusive, which designates the set of all divisors of n^2.