Number Theory

University of Manitoba, Mathletics 2009

1 Facts and definitions

Modular Arithmetic: Let a, b, and m be integers, with $m \neq 0$. We say that a and b are congruent modulo m if m divides $a - b$. We denote this by $a \equiv b \pmod{m}$.
Properties:

- $a \equiv a \pmod{m}$ (reflexivity).
- If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$ (transitivity).
- If $a \equiv b \pmod{m}$, then $b \equiv a \pmod{m}$.
- If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a + c \equiv b + d \pmod{m}$ and $a - c \equiv b - d \pmod{m}$.
- If $a \equiv b \pmod{m}$, then for any integer k, $ka \equiv kb \pmod{m}$.
- If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $ac \equiv bd \pmod{m}$. In general, if $a_i \equiv b_i \pmod{m}$, $1 \leq i \leq k$, then $a_1 \dots a_k \equiv b_1 \dots b_k \pmod{m}$. In particular, if $a \equiv b \pmod{m}$, then for any positive integer k, $a^k \equiv b^k \pmod{m}$.
- If $m_1, \dots, m_k$ are pairwise relatively prime, then $a \equiv b \pmod{m_i}$, $1 \leq i \leq k$, if and only if $a \equiv b \pmod{m_1 \dots m_k}$.
- Cancellation rule: if $gcd(c, m) = 1$ and $ca \equiv cb \pmod{m}$, then $a \equiv b \pmod{m}$.
- Let m be a positive integer, and let a, b, and c be integers with $c \neq 0$. If $ac \equiv bc \pmod{m}$, then
$$a \equiv b \left(\mod \frac{m}{gcd(c, m)} \right).$$

Fact: if $gcd(a, m) = 1$, then there is x such that $ax \equiv 1 \pmod{m}$. We call such x the inverse of a modulo m. The inverse of a is uniquely determined (or well defined) modulo m for all integers relatively prime to m.

Euler's totient function: For any positive integer m we denote by $\phi(m)$ the number of all positive integers n less than m that are relatively prime to m. (Note: $\phi(2) = 1$, $\phi(3) = 2$, $\phi(4) = 2$, $\phi(p) = p - 1$, for any prime p.)

Euler's Theorem: Let a and m be relatively prime positive integers. Then $a^{\phi(m)} \equiv 1 \pmod{m}$.

Fermat's Little Theorem:
Let a be a positive integer and let p be a prime. Then $a^p \equiv a \pmod{p}$.

Theorem: If $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ is the prime factorization of $n > 1$, then

$$\phi(n) = n \left(1 - \frac{1}{p_1}\right) \dots \left(1 - \frac{1}{p_k}\right) .$$

Prime Number Theorem: Let $\pi(n)$ denote the number of primes less than or equal to n. Then

$$\lim_{n \to \infty} \frac{\pi(n)}{n/\ln n} = 1 .$$

Bézout's Theorem:
For positive integers m and n, there exist integers x and y such that $mx + ny = gcd(m, n)$.

Fact (sum of divisors): For a positive integer n denote by $\sigma(n)$ the sum of its positive divisors, including 1 and n itself. It is clear that $\sigma(n) = \sum_{d|n} d$.
If $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ is the prime factorization of n, then

$$\sigma(n) = \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \dots \frac{p_k^{\alpha_k+1} - 1}{p_k - 1} .$$

Idea: Each divisor of n appears exactly once in the expansion of the product

$$(1 + p_1 + \dots + p_1^{\alpha_1}) \dots (1 + p_k + \dots + p_k^{\alpha_k}) .$$

Legendre's formula: The exponent of p in the prime factorization of $n!$ is

$$e_p(n!) = \sum_{r \geq 1} \left\lfloor \frac{n}{p^r} \right\rfloor .$$

Sophie Germain identity: $a^4 + 4b^4 = (a^2 + 2b^2)^2 - (2ab)^2 = (a^2 + 2b^2 + 2ab)(a^2 + 2b^2 - 2ab)$.

2 Examples

Example 4.1: Is it possible to write 1 as a sum of reciprocals of 2010 odd integers?
Solution: Suppose that the answer is "yes", and so we can find $k := 2010$ odd integers $n_1, \dots, n_k$ such that

$$1 = \frac{1}{n_1} + \dots + \frac{1}{n_k} .$$

Multiplying this equation by $n_1 \dots n_k$ we get

$$n_1 \dots n_k = s_1 + \dots + s_k ,$$

where $s_i = n_1 \dots n_{i-1} n_{i+1} \dots n_k$, $1 \leq i \leq k$. Since any product of odd integers is odd, and the sum of an even number of odd integers is even, we conclude that the left-hand side of the last displayed equation is odd but its right-hand side is even, which is a contradiction. Hence, our assumption that the answer is "yes" is wrong.

Example 4.2: Find all primes such that $p + q = (p - q)^3$.
Solution: First, note that p cannot be equal to q. Since $p - q \equiv 2p \pmod{p+q}$, we have $(p-q)^3 \equiv 8p^3 \pmod{p+q}$, but $(p-q)^3 \equiv 0 \pmod{p+q}$, and so $8p^3 \equiv 0 \pmod{p+q}$. Now, p and $p+q$ are relatively prime ($gcd(p, p+q) = 1$), and so $gcd(p^3, p+q) = 1$. Therefore, $8 \equiv 0 \pmod{p+q}$. Also, $p + q \equiv (p-q)^3 \equiv 0 \pmod{p-q}$, and so $(p+q) + (p-q) = 2p \equiv 0 \pmod{p-q}$. Since p and $p-q$ are relatively prime, this implies that $2 \equiv 0 \pmod{p-q}$, i.e., $p - q$ divides 2. It is now easy to check that $p = 5$ and $q = 3$ is the only possibility.

Example 4.3: Consider the prime numbers $n_1 < n_2 < \cdots < n_{31}$. Prove that if 30 divides $n_1^4 + \ldots n_{31}^4$, then among these numbers one can find three consecutive primes.
Solution: Let $s := n_1^4 + \ldots n_{31}^4$ Firstly, we claim that $n_1 = 2$. Otherwise, all numbers n_i, $1 \leq i \leq 31$, are odd, and consequently s is odd, a contradiction. Secondly, we claim that $n_2 = 3$. Otherwise, we have $n_i^4 \equiv 1 \pmod 3$ for all $1 \leq i \leq 31$ (since $n_i \equiv \pm 1 \pmod 3$). Therefore, $s = n_1^4 + \ldots n_{31}^4 \equiv 31 \equiv 1 \pmod 3$, a contradiction. Finally, we prove that $n_3 = 5$. Indeed, if not, then $n_i \equiv \pm 1 \pmod 5$ or $n_i \equiv \pm 2 \pmod 5$, and so $n_i^2 \equiv \pm 1 \pmod 5$ which implies that $n_i^4 \equiv 1 \pmod 5$ and, again, we get a contradiction.

We conclude that three consecutive primes, namely, 2, 3, and 5, appear in the given prime numbers.

Example 4.4 (Wilson's Theorem): For any prime p, $(p-1)! \equiv -1 \pmod p$.
Proof: The property holds for $p = 2$ and $p = 3$, so we may assume that $p \geq 5$. Let $S = \{2, 3, \ldots, p-2\}$. Because p is prime, for any $s \in S$, s has a unique inverse $s' \in \{1, 2, \ldots, p-1\}$. Moreover, $s' \neq 1$ and $s' \neq p-1$, and so $s' \in S$. In addition, $s' \neq s$; otherwise, $s^2 \equiv 1 \pmod p$, implying $p|(s-1)$ or $p|(s+1)$, which is not possible, since $s + 1 < p$. It follows that we can group the elements of S in $(p-3)/2$ distinct pairs (s, s') such that $ss' \equiv 1 \pmod p$. Multiplying these congruences gives $(p-2)! \equiv 1 \pmod p$ and the conclusion follows.

3 Problems for discussion

Discussion problem 4.1: Prove that, for any $n \geq 2$, $n^4 + 4^n$ is never a prime number.

Discussion problem 4.2: Prove that the equation $15x^2 - 7y^2 = 9$ has no integer solutions.

Discussion problem 4.3: Let α and β be positive irrational numbers such that $1/\alpha + 1/\beta = 1$. Then the sequences $f(n) = \lfloor \alpha n \rfloor$ and $g(n) = \lfloor \beta n \rfloor$, $n \in \mathbb{N}$, are disjoint and their union is $\mathbb{N}$.

Discussion problem 4.4: Find 2009 consecutive composite integers.

Discussion problem 4.5: Find the number of terminal zeros in the decimal representation of 1000!.

4 Solutions for discussion problems

Discussion problem 4.1: Prove that, for any $n \geq 2$, $n^4 + 4^n$ is never a prime number.
Solution: If n is even, then $n^4 + 4^n$ is even and larger than 2, and so is not a prime. If $n = 2k + 1$, then $n^4 + 4^n = n^4 + 4 \cdot 4^{2k} = n^4 + 4 \cdot (2^k)^4$, and so has the form $a^4 + 4b^4$, and so is not a prime by Sophie Germain's identity.

Discussion problem 4.2: Prove that the equation $15x^2 - 7y^2 = 9$ has no integer solutions.
Solution: Clearly, $y = 3y_1$, and $15x^2 - 63y_1^2 = 9 \Rightarrow 5x^2 - 21y_1^2 = 3$, and so $x = 3x_1$. Hence, $45x_1^2 - 21y_1^2 = 3 \Rightarrow 15x_1^2 - 7y_1^2 = 1 \Rightarrow 7y_1^2 \equiv -1 \pmod 3 \Rightarrow y_1^2 \equiv -1 \pmod 3$ which cannot happen since $y_1^2 \equiv 0$ or $1 \pmod 3$.

Discussion problem 4.3: Let α and β be positive irrational numbers such that $1/\alpha + 1/\beta = 1$. Then the sequences $f(n) = \lfloor \alpha n \rfloor$ and $g(n) = \lfloor \beta n \rfloor$, $n \in \mathbb{N}$, are disjoint and their union is $\mathbb{N}$.
Solution: Sequences are disjoint. Otherwise, $\lfloor \alpha m \rfloor = \lfloor \beta n \rfloor = q$, and so $q < \alpha m < q + 1$ and $q < \beta n < q + 1$ (since α and β are irrational). Therefore,

$$\frac{m}{q+1} < \frac{1}{\alpha} < \frac{m}{q} \quad \text{and} \quad \frac{n}{q+1} < \frac{1}{\beta} < \frac{n}{q}\,.$$

Adding these inequalities, we get

$$\frac{m+n}{q+1} < 1 < \frac{m+n}{q} \quad \Rightarrow \quad q < m + n < q + 1\,,$$

which is a contradiction. Thus, $\lfloor \alpha m \rfloor \neq \lfloor \beta n \rfloor$.

Observe that α and β are both greater than one and cannot be both greater than 2. Hence, on of these numbers is in $(1, 2)$. Suppose now that there exists $q \in \mathbb{N}$ which does not appear in the union of the sets $\{f(n)\}$ and $\{g(n)\}$. Therefore, $\forall k \in \mathbb{N}, \alpha k \notin (q, q + 1)$ and $\beta k \notin (q, q + 1)$. Let $m, n \in \mathbb{N}$ be such that

$$\alpha m < q < q + 1 < \alpha(m + 1) \quad \text{and} \quad \beta n < q < q + 1 < \beta(n + 1)\,.$$

Hence,

$$\frac{m}{q} < \frac{1}{\alpha} < \frac{m+1}{q+1} \quad \text{and} \quad \frac{n}{q} < \frac{1}{\beta} < \frac{n+1}{q+1}$$

and so

$$\frac{m+n}{q} < 1 < \frac{m+n+2}{q+1} \quad \Rightarrow \quad m+n < q < q+1 < m+n+2 \quad \Rightarrow \quad m+n < q < m+n+1\,,$$

which is again a contradiction.

Discussion problem 4.4: Find 2009 consecutive composite integers.
Solution: Note that $n! + 2, n! + 3, \ldots, n! + n$ are $(n - 1)$ consecutive composite integers. Now, take $n = 2010$.

Discussion problem 4.5: Find the number of terminal zeros in the decimal representation of 1000!.

Solution: Using Legendre's formula, we can find the exponent of 5 in the prime factorization of 1000!:

$$e_5(1000!) = \sum_{r\geq 1} \left\lfloor \frac{1000}{5^r} \right\rfloor = \left\lfloor \frac{1000}{5} \right\rfloor + \left\lfloor \frac{1000}{25} \right\rfloor + \left\lfloor \frac{1000}{125} \right\rfloor + \left\lfloor \frac{1000}{625} \right\rfloor = 200 + 40 + 8 + 1 = 249\,.$$

The exponent of 2 in the prime factorization of 1000! is

$$e_2(1000!) = \sum_{r\geq 1} \left\lfloor \frac{1000}{2^r} \right\rfloor = \left\lfloor \frac{1000}{2} \right\rfloor + \left\lfloor \frac{1000}{4} \right\rfloor + \cdots > 249\,.$$

Hence, the number of terminal zeros in the decimal representation of 1000! is 249.

5 Take home problems

Take home problem 4.1: Prove that there is no polynomial $p(x)$ of degree ≥ 1 such that, for all positive integers n, $p(n)$ is a prime number.

Take home problem 4.2: Find the last three digits of the number 2009^{2010}.

Take home problem 4.3: Find the last three digits of the number $2009^{2008^{2007}}$.

6 Take home solutions

Take home problem 4.1: Prove that there is no polynomial $p(x)$ of degree ≥ 1 such that, for all positive integers n, $p(n)$ is a prime number.
Solution: Suppose that there is such a polynomial $p(x)$, and that its degree is $n \geq 1$. Considering $x = 1, 2, \ldots, n+1$ and using the fact that the Vandermonde matrix is non-singular, we conclude that $p(x)$ has to have rational coefficients. Hence, by multiplying $p(x)$ by the LCM of the coefficients (call it L), we conclude that there is a polynomial $q(x)$ of degree n with integer coefficients such that $q(n) = r_n L$, $n \geq 1$, where r_n's are all prime and $L \in \mathbb{N}$.

Denote $q(1) = r_1 L =: M$ and consider $q(1 + kM)$, $k \in \mathbb{N}$. Since $kM \,|\, (q(1 + kM) - q(1))$, we conclude that $M \,|\, q(1 + kM)$ and hence $r_1 | r_{1+kM}$, for all $k \in \mathbb{N}$. This can only happen if $r_{1+kM} = \pm r_1$ for all $k \in N$ and, in particular, for $1 \leq k \leq 2n + 1$. By the PHP, there are $n + 1$ values of k such that r_{1+kM} are the same (and are equal to r_1 or $-r_1$). Therefore, the polynomial $q(x)$ of degree n assumes the same value at $n + 1$ points, which can only happen if $q(x)$ is constant, and so $n = 0$. Contradiction.

Take home problem 4.2: Find the last three digits of the number 2009^{2010}.
Solution: First of all,

$$2009^{2010} \equiv 9^{2010} \pmod{1000}$$

Since 9 and 1000 are relatively prime, by Euler's theorem, we have $9^{\phi(1000)} \equiv 1 \pmod{1000}$. Since $1000 = 2^3 \cdot 5^3$, we have $\phi(1000) = 1000 \times (1 - 1/2) \times (1 - 1/5) = 400$, and so $9^{400} \equiv 1 \pmod{1000}$. Hence, $9^{2000} = (9^{400})^5 \equiv 1 \pmod{1000}$. Therefore, $9^{2010} \equiv 9^{10} \pmod{1000}$. Now,

$$\begin{aligned} 9^{10} &= (10-1)^{10} = \sum_{i=0}^{10} \binom{10}{i} 10^i (-1)^{10-i} = (-1)^{10} + \binom{10}{1} 10(-1)^9 + \binom{10}{2} 10^2 (-1)^8 + 1000A \\ &= 1 - 100 + 4500 + 1000A \end{aligned}$$

and so $9^{10} \equiv 4401 \equiv 401 \pmod{1000}$. Hence, 2009^{2010} ends with 401.

Take home problem 4.3: Find the last three digits of the number $2009^{2008^{2007}}$.
Solution: As above, $\phi(1000) = 1000 \times (1 - 1/2) \times (1 - 1/5) = 400$, $9^{400} \equiv 1 \pmod{1000}$, and

$$2009^m \equiv 9^m \pmod{1000},$$

where $m = 2008^{2007}$. Now, we determine $n < 400$ such that $m \equiv n \pmod{400}$. Then, since $m = n + 400k$, $9^m \equiv 9^n \cdot (9^{400})^k \equiv 9^n \pmod{1000}$.

Now, clearly $2008^{2007} \equiv 8^{2007} \pmod{400} \equiv 2^{6021} \pmod{400}$. Since $400 = 25 \cdot 16$ and $16 | 2^{6021}$, we know that $m \equiv 2^{6021} \equiv 2^4 k \pmod{400}$, and so

$$2^{6017} \equiv k \pmod{25}.$$

Since $\phi(25) = 25 \times (1 - 1/5) = 20$, Euler's theorem implies $2^{20} \equiv 1 \pmod{25}$, and so

$$2^{6017} \equiv 2^{6020} \cdot 2^{-3} \equiv 22 \pmod{25},$$

and so $k = 22$. Hence, $m \equiv 16 \cdot 22 \equiv 352 \pmod{400}$, and so $n = 352$. Therefore,

$$2009^{2008^{2007}} \equiv 9^{352} \pmod{1000}.$$

Now,

$$\begin{aligned} 9^{352} &= (10-1)^{352} = \sum_{i=0}^{352} \binom{352}{i} 10^i (-1)^{352-i} = 1 - \binom{352}{1} 10 + \binom{352}{2} 10^2 + 1000A \\ &= 1 - 3520 + 176 \cdot 351 \cdot 100 + 1000A = -3519 + 100(170+6)(350+1) + 1000A\,, \end{aligned}$$

i.e.,

$$9^{352} \equiv -519 + 600 \equiv 81 \pmod{1000}\,,$$

and we conclude that $2009^{2008^{2007}}$ ends with 081.

References

[1] Titu Andreescu, Dorin Andrica, and Zuming Feng, *104 number theory problems*, Birkhäuser Boston Inc., Boston, MA, 2007. From the training of the USA IMO team. MR2281653 (2007g:11001)

[2] Arthur Engel, *Problem-solving strategies*, Problem Books in Mathematics, Springer-Verlag, New York, 1998. MR1485512 (98m:00004)

[3] Edward Lozansky and Cecil Rousseau, *Winning solutions*, Problem Books in Mathematics, Springer-Verlag, New York, 1996. MR1415836 (97j:00003)