Introduction to Advanced Modular Arithmetic

David Tang

January 2019

0 Introduction

Our guiding question is: What is modular arithmetic?

To answer this question, we must first investigate what remainders are for integers.

A remainder of p/q is the number obtained by subtracting q from p until further subtraction will result in a negative number. Thus, the remainder is always in the range $[0, q-1]$.

Notice that this definition only works for non-negative integers p, q. Let us say that p is negative. Then, we may define the remainder as the negative of the remainder of $-p/q$. This remainder is always in the range $[-q+1, 0]$. This number can also be defined by adding q to p until further addition will result in a positive number.

Using this variability in either adding or subtracting, we may now define the remainder for negative integers q. Instead of subtracting by q if p is positive, we may instead add q, and vice versa for a negative p. Thus, we can now define the remainder of any fraction p/q of integers.

Disclaimer: These definitions are highly contentious and some may argue that if q is negative, it means we want the remainder from the range $[q+1, 0]$ of $p/-q$, meaning we take q plus the remainder of $p/-q$.

There are infinite integers that may have the same remainder upon division by a fixed number q using this method. For example, if we wish to obtain a remainder of 2 and $q = 3$, numbers from the set $S = \{2, 5, 8, 11, \cdots\}$ will work. If you can find any one of these numbers, you can obtain the rest by adding or subtracting q. Through this definition, we may merge the two sets $S_1 = \{-1, -4, -7, \cdots\}$ with $S_2 = \{2, 5, 8, \cdots\}$ if $q = 3$ as we can get from one to another by subtracting or adding 3. Thus, we notice that the remainder r and $r - q$ are equivalent. From here, we can conjecture that a certain number q will only have q distinct sets for which each set contains all integers whose remainder is equivalent upon division by q.

Now, introducing the modulo notation, if a_1, a_2 are two elements in one of the aforementioned sets, then $a_1 \equiv a_2 \pmod{q}$. You say this as a_1 is congruent or equivalent to a_2 modulo q. q is known as the modulus of the congruence. On the topic of introducing new terminology, the set that we mentioned

earlier is known as the congruence or residue class of an integer a modulo q

There is another way to see the congruence relation. If we use a 12-hour clock, assuming we don't peek at the clock, we would not be able to tell the difference between $2, 14, 26, \cdots$ hours passing. Heck, we don't even know if we might have travel back in time by 10 hours. Thus, these different amounts of time are congruent in the case of a 12-hour clock. Also, notice that from this example the loss of information. Knowing that $a \equiv b \pmod{c}$ doesn't give as much information as $a = b$.

Through this lecture, I intend to develop the basic theory behind Modular Arithmetic from scratch and introduce you to some concepts in advanced Modular Arithmetic, including quadratic residues and primitive roots. Also, I will demonstrate how to use it to solve problems in math contests ranging from AMC difficulty to USAMO difficulty.

1 Basic Properties

There are many interesting properties of the congruence relation. The following list contains all important ones. It is left as an exercise to the reader to prove these.

1. $a \equiv a \pmod{n}$
2. $a \equiv b \pmod{n}$ if and only if $b \equiv a \pmod{n}$
3. If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$.
4. If $a \equiv b \pmod{n}$, then
   (a) $a + c \equiv b + c \pmod{n}$ for any integer c
   (b) $ca \equiv cb \pmod{n}$ for any integer c
   (c) $a^c \equiv b^c \pmod{n}$ for any non-negative integer c
   (d) $p(a) \equiv p(b) \pmod{n}$ for any polynomial $p(x)$ with integer coefficients.
5. If $a_1 \equiv b_1 \pmod{n}$ and $a_2 \equiv b_2 \pmod{n}$, then
   (a) $a_1 + a_2 \equiv b_1 + b_2 \pmod{n}$
   (b) $a_1 - a_2 \equiv b_1 - b_2 \pmod{n}$
   (c) $a_1 a_2 \equiv b_1 b_2 \pmod{n}$

2 Three Most Important Theorems

Along with these basic properties, I will present three really important theorems about modular arithmetic.

1. (Wilson's Theorem) $(p-1)! \equiv -1 \pmod{p}$ if and only if p is prime.

2. (Fermat's Little Theorem) If p is prime, $a^{p-1} \equiv 1 \pmod{p}$
3. (Euler's Theorem) This is a generalization of Fermat's Little Theorem. If $gcd(a, n) = 1$, $a^{\varphi(n)} \equiv 1 \pmod{n}$, where $\varphi(x)$ is the number of integers i from 1 to $x - 1$ such that $gcd(i, x) = 1$.

3 Rational Numbers

Let us investigate rational numbers in modular arithmetic. Specifically, we seek to define $\frac{b}{a} \pmod{n}$. Let us assume that $\frac{b}{a}$ is in its most simplified state so $gcd(b, a) = 1$. Surprisingly, we can find that $\frac{b}{a} \equiv$ an integer $\pmod{n}$ if $gcd(a, n) = 1$. Let $\frac{b}{a} \equiv c \pmod{n}$. Then, $b \equiv ac \pmod{n}$ or $b - ac \equiv 0 \pmod{n}$. Obviously, b must divide $gcd(a, n)$ if this is to be true. Since $gcd(b, a) \equiv 1$, $gcd(b, gcd(a, n)) = 1$. Thus, $gcd(a.n) = 1$ if and only if b is to divide $gcd(a, n)$, so c is undefined if $gcd(a, n) \neq 1$. Now, we may notice that we may substitute b, a, c with any integer in their residue class. The proof is as follows (which I present to show a common way to solve properties modulo n):

A standard way to prove results modulo n is to make the equation equivalent to zero on one side and then substitute each number k with $k + x_k n$. If a and b are in the same residue class, then $a \equiv b \pmod{n}$, or $a = b + x_a n$ for an integer x_a. Thus, we may change the above condition to proving that $b - ac \equiv 0 \pmod{n} \iff b + x_b n - (a + x_a n)(c + x_c n) \equiv 0 \pmod{n}$. Now, notice that $b + x_b n - (a + x_a n)(c + x_c n) \equiv b - ac + n(x_b - x_a - x_c - n x_c x_b) \equiv b - ac \pmod{n}$. Thus, we arrive at our conclusion that $b - ac \equiv 0 \pmod{n} \iff b + x_b n - (a + x_a n)(c + x_c n) \equiv 0 \pmod{n}$ since $b - ac \equiv b + x_b n - (a + x_a n)(c + x_c n) \pmod{n}$.

Now, let us take a look at modular multiplicative inverses, or basically $a^{-1} \pmod{n}$. In short, we call this number the inverse of a modulo n. Using the above property, if there exists a possible solution for this number, there must exist a solution from $[0, n - 1]$ as we may subtract n until we reach a number in this range. We may prove that such an integer exists if $gcd(a, n) = 1$. From Euler's Theorem, $a^{\varphi(n)} \equiv 1 \pmod{n}$. Thus, $a^{\varphi(n)-1} \equiv a^{-1} \pmod{n}$. As a result, we get that $a^{-1} \equiv a^{\varphi(n)-1} \pmod{n}$, so if a is an integer such that $gcd(a.n) = 1$, a always has a modular inverse modulo n. Notice how this is cyclic, because the inverse of $a^{-1} \pmod{n}$ is just a. Now, let us prove that $a^{-1} \pmod{n}$ can only take values in a single residue class modulo n. By contradiction, let us assume it takes values in two different residue classes. Thus, $a^{-1} \equiv b \equiv c \pmod{n}$, where $b \neq c$ and $0 \leq b, c \leq n - 1$. Thus, $b - c \equiv 0 \pmod{n}$. We arrive at a contradiction because it is impossible to pick two distinct numbers from the set of integers between 0 and $n - 1$ such that their difference is a multiple of n, so our contradiction hypothesis must be false. Thus, $a^{-1} \pmod{n}$ can only take values from a single residue class modulo n.

Arriving back at our original question, we may notice that if $\frac{b}{a} \equiv c \pmod{n}$, then $c \equiv ba^{-1} \pmod{n}$. Since a^{-1} will always have a possible value from exactly one residue class modulo n, we get that there exists a value c from exactly one residue class modulo n because $c \equiv ba^{-1} \pmod{n}$, so adding a multiple of n to a^{-1} is equivalent to adding a multiple of n to c. Thus, we have shown that $\frac{b}{a} \equiv ba^{\varphi(n)-1} \pmod{n}$.

4 AMC, AIME, CEMC Level Problems

In no particular order:

1. (Own) Find the remainder when we divide $6^{41} + 8^{41}$ by 49.
2. (AMC 12 A 2017) Let $S(n)$ equal the sum of the digits of positive integer n. For example, $S(1507) = 13$. For a particular positive integer n, $S(n) = 1274$. Which of the following could be the value of $S(n+1)$?
   (A) 1 **(B)** 3 **(C)** 12 **(D)** 1239 **(E)** 1265
3. (Hypatia 2018) A sequence $T_1, T_2, T_3, \cdots$ is defined by $T_1 = 1, T_2 = 2$, and each term after the second is equal to 1 more than the product of all previous terms in the sequence. That is, $T_{n+1} = 1 + T_1T_2T_3 \cdots T_n$ for all integers $n \geq 2$. For example, $T_3 = 1 + T_1T_2 = 3$. Prove that T_{2018} is not a perfect square.
4. (AHSME 1992) The 2-digit integers from 19 to 92 are written consecutively to form the integer $N = 192021 \cdots 9192$. Suppose that 3^k is the highest power of 3 that is a factor of N. What is k?
5. (AIME II 2004) Let S be the set of integers between 1 and 2^{40} whose binary expansions have exactly two 1's. If a number is chosen at random from S, the probability that it is divisible by 9 is p/q, where p and q are relatively prime positive integers. Find $p + q$.
6. (Own) Prove that $2^{2n} + 10 \cdot 15^n$ is always divisible by 11.
7. (CSMC 2018) Let $f(n)$ be the number of strings of length n with characters from the set A, B, C such that
   - CC occurs as a substring, and
   - if either AB or BA occurs as a substring then there is an occurrence of the substring CC to its left.

   (For example, when n = 6, the strings CCAABC and ACCBBB and CCABCC satisfy the requirements, but the strings BACCAB and ACBBAB and ACBCAC do not.) Prove that $f(2097)$ is a multiple of 97.
8. (AIME I 2017) Let $a > 1$ and $x > 1$ satisfy $\log_a(\log_a(\log_a 2) + \log_a 24 - 128) = 128$ and $\log_a(\log_a x) = 256$. Find the remainder when x is divided by 1000.
9. (AMC 12 B 2017) Let $N = 123456789101112 \ldots 4344$ be the 79-digit number that is formed by writing the integers from 1 to 44 in order, one after the other. What is the remainder when N is divided by 45?
10. (AIME I 2014) The positive integers N and N^2 both end in the same sequence of four digits $abcd$ when written in base 10, where digit a is not zero. Find the three-digit number abc.

5 Look at Equations Modulo n

Let us look at the following problem:

Find all solutions for positive integers x, y, z to $7x^2 + 4y^2 = 3z^2$.

Trying out numbers makes us notice that there appears to be no solution to this system of equations. But how do we prove this? I will show you a proof involving two very important topics in questions surrounding modular arithmetic. The first is simply that taking the value of both sides of an equality modulo n still maintains that equality as an equivalency. Secondly, the method of infinite descent, where if we can prove that all variables in an equation is divisible by a number greater than one, and the equation is homogeneous (same power for all variables), then there are no solutions in the positive (or negative) integers.

Noticing the 3 coefficient in front of the z, we may take this equation modulo 3. Thus, we get that $7x^2+4y^2 \equiv 3z^2 \pmod 3$. By taking each of the coefficients modulo 3, we get that $x^2+y^2 \equiv 0 \pmod 3$. Now, we notice that all perfect squares must be 0 or 1 modulo 3 by trying out the squares of all numbers from 0 to 2, since all other numbers are equivalent to one of these numbers modulo 3. Thus, the only way to make $x^2+y^2 \equiv 0 \pmod 3$ is if $x \equiv y \equiv 0 \pmod 3$. Since both x and y are 0 modulo 3, we can write $x = 3x'$ and $y = 3y'$ for positive integers x', y'. Thus, $7(3x')^2+4(3y')^2 = 3z^2 \iff 9(7x'^2+4y'^2) = 3z^2$. Now, taking the equation modulo 9, we get that $3z^2 \equiv 0 \pmod 9$. Thus, by checking all possible remainders for z modulo 9, we get that $z \equiv 0, 3, 6 \pmod 9$ or $z \equiv 0 \pmod 3$. Thus, if $7x^2 + 4y^2 = 3z^2$, then $7(3x')^2 + 4(3y')^2 = 3(3z')^2$ where $x = 3x', y = 3y', z = 3z'$. This simplifies to $7x'^2 + 4y'^2 = 3z'^2$.

Now, we can move on to our infinite descent part of the proof. Let x_0, y_0, z_0 be the solution with the minimum value x_0 to our problem. We have proven that if $7x^2+4y^2 = 3z^2$, then $7x'^2+4y'^2 = 3z'^2$ must be a solution where $x = 3x', y = 3y', z = 3z'$. Thus, x', y', z' is also a solution. Yet, $x' = \frac{x}{3} < x$, so we get a contradiction. Thus, there can never be a solution to our problem that minimizes x_0, or the value of x_0 can infinitely decrease (hence the name infinite descent). Yet, since x_0 has a minimum bound as it is a positive integer, we must have a minimum value of x_0 if there are a non-zero amount of solutions. Thus, no solutions exist to this equation.

Now, we have a taste of an Olympiad-style problem from Canada Math Camp 2018.

Find all functions $f : \mathbb{N} \to \mathbb{N}$ (where $\mathbb{N}$ includes 0) such that:

$$xf(y) + yf(x) = (x + y)f(x^2 + y^2) \ \forall x, y \in \mathbb{N}$$

How would we approach this problem? First, we can try special cases. Let us try $y = 0$. We get that $xf(0) = xf(x^2) \iff f(0) = f(x^2) \ \forall x \in \mathbb{N}$. At this point, most of us (including me) would get stuck for at least ten minutes. Attempting to prove any other properties of $f(x)$ using only the equation provided gets you nowhere.

Noticing that $f(x) \in \mathbb{N}$, we are motivated to look at this equation modulo $x + y$. Thus, we get that $xf(y) + yf(x) \equiv (x + y)f(x^2 + y^2) \equiv 0 \equiv (x + y)f(x) \pmod{x + y}$. Then, we can obtain that $xf(y) \equiv xf(x) \pmod{x + y}$. Choosing $x = a$ and $y = b^2$, where $gcd(b, a) = 1$, we can get that $af(b^2) \equiv af(a) \pmod{a + b^2}$ or $f(a) \equiv f(0) \pmod{a + b^2}$. Now, we can fix the value for a and vary the value of b across all positive integers co-prime to a of which there are infinite possibilities. Thus, we establish that $f(a) \equiv f(0) \pmod n$ for a set of infinite values of n. Logically, this means that

$f(a) = f(0)$ so we have proven that, for all values of x, $f(x) = f(0)$. Thus, $f(x) = c$ for any value $c \in \mathbb{N}$, which we can verify satisfies our original equation. A rigorous proof for our final step can be given in the following manner:

Proof by contradiction:

Assume there is a value for a such that $f(a) \neq f(0)$. Let $f(a) = m$ and $f(0) = n \neq m$. We know that $m - n \equiv 0 \pmod{a + b^2}$. Since $m - n$ is finite, there will always exist a value b co-prime to a such that $a + b^2 > |m - n|$. This can be written as $-a - b^2 < m - n < a + b^2$. Since the only value in this range that is equivalent to 0 $\pmod{a + b^2}$ is 0, $m - n = 0$ or $m = n$. Thus, we arrive at a contradiction so there does not exist a value for a such that $f(a) \neq f(0)$.

6 Primitive Roots

Let us take a look at primitive roots. Let us say we have an integer x and we wish to investigate all possible values that x^k, where k is an integer, can take modulo n. Since this equation is periodic with a period of $\varphi(n)$ as $x^{\varphi}(n) \equiv 1 \pmod{n}$, we may notice that all of the possible values modulo n is equal to all of the possible values created when $0 \leq k \leq \varphi(n) - 1$. Since $x^k = 1$ and if $x^{k_1} \equiv x^{k_2} \pmod{n}$, then $x^{k_1 - k_2} \equiv 1 \pmod{n}$, all possible periods must be a factor of $\varphi(n)$ and the period is equal to the smallest positive integer k such that $x^k \equiv 1 \pmod{n}$.

Now, let us define a primitive root. A primitive root modulo n is a number x such that the period of x^k is equal to $\varphi(n)$. In fact, since the definition of $\varphi(n)$ is the number of integers that are less than n which are co-prime to n, a primitive root can be defined a second way: x is a primitive root if and only if there exists a k for every integer a co-prime to n such that $x^k \equiv a \pmod{n}$. This is because any primitive root x^k must cycle through all $\varphi(n)$ elements as it cannot repeat and it cannot take any values that are not co-prime to n if x is co-prime to n.

Now, let us define two useful functions that are related to primitive roots. The first is the Carmichael function, $\lambda(n)$. It is defined as the smallest integer m such that $a^m \equiv 1 \pmod{n}$ for every integer a between 1 and $n - 1$ inclusive that is co-prime to n. Notice that if $\lambda(n) < \varphi(n)$ (but not the other way around!), then n can never have a primitive root as all periods will be at most $\lambda(n)$.
Another interesting function is the Mobius function, $\mu(n)$. This is very similar to the Legendre symbol (which is a function that will be discussed in the next part about quadratic residues) as it only takes a value from the set $-1, 0, 1$ and is multiplicative, which means $\mu(a) * \mu(b) = \mu(ab)$.

The definition of $\mu(n)$ is:

$$\mu(n) = \begin{cases} 1 & \text{if } n \text{ is a square-free positive integer with an even number of prime factors} \\ 0 & \text{if } n \text{ has a squared prime factor} \\ -1 & \text{if } n \text{ is a square-free positive integer with an odd number of prime factors.} \end{cases}$$

Now, using this function, we can find the product and the sum of all primitive roots of an integer p, where p is prime. The product of all primitive roots are 1 $\pmod{p}$ if $p \neq 3$ and $-1 \pmod{p}$ if $p = 3$. The sum of all primitive roots are $\mu(p - 1) \pmod{p}$. Again, this has many parallels with quadratic residues and the Legendre symbol. The proofs of these are left to the reader.

7 Quadratic Residues

Let us take a look at quadratic residues after hyping it up so much in the last chapter.

We may define a quadratic residue q modulo n as a value q such that there exists an integer x where $x^2 \equiv q \pmod{n}$. The opposite of a quadratic residue is a quadratic non-residue. (I will refer to them interchangeably as a quadratic residue and a residue in this section) First of all, it is obvious that we can find all possible quadratic residues by finding all possible residues of 0^2, 1^2, 2^2, $\cdots$, $\lfloor \frac{n}{2} \rfloor^2$ modulo n. This is because quadratic residues are symmetric about $\frac{n}{2}$ as $-x^2 = x^2$. Thus, there is a maximum of $\lfloor \frac{n}{2} \rfloor + 1$ distinct residues modulo n. Also, it is key to notice that the set of all quadratic residues modulo a prime p is closed under multiplication or division, meaning if you divide or multiply two or more residues, you also get another residue. Most of the time, residues are integers from $-n+1$ to $n-1$ since we have proven in all earlier parts that any rational number is equivalent to an integer in the range 0 to $n-1$. Thus, the multiplicative inverse of a residue is a residue and the multiplicative inverse of a non-residue is a non-residue modulo a prime p as 1 is always a residue modulo p. The proof of these statements is left to the reader.

One of the most important theorems is the Law of Quadratic Reciprocity. It states that for an odd prime p, -1 is a residue modulo p if and only if $p \equiv 1 \pmod{4}$. And x is a residue modulo p and $-x$ is a residue modulo p if and only if -1 is a residue modulo p. This is a direct consequence of the set of residues modulo a prime p being closed under division.

Now we can introduce the use of Legendre Symbols. The Legendre Symbol represents whether a number a is a quadratic residue modulo a prime p and is defined as follows.

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue modulo } p \text{ and } a \not\equiv 0 \pmod{p}, \\ -1 & \text{if } a \text{ is a quadratic non-residue modulo } p, \\ 0 & \text{if } a \equiv 0 \pmod{p}. \end{cases}$$

Two important theorems makes the computation of the value of a Legendre Symbol faster than brute force. First, the Legendre Symbol of two numbers with the same bottom value p is completely multiplicative, so the function value of the product is the same as the product of the two function values for any two not necessarily co-prime integers. Second, we have the Law of Quadratic Reciprocity, which was proven by Gauss. For two distinct odd prime integers p and q:

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

Two additional equations that are needed to help this law are:

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4 \\ -1 & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

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

To give an example of how to use this formula:

$$\left(\frac{12345}{331}\right) = \left(\frac{98}{331}\right) = \left(\frac{2 \cdot 7^2}{331}\right) = \left(\frac{2}{331}\right) = (-1)^{\frac{331^2-1}{8}} = -1.$$

Thus, 12345 is a non-residue modulo 331.

8 Key Advanced Theorems

Also, we may state many famous theorems and properties involving the modulo n notation.

1. (Chinese Remainder Theorem) If $x \equiv a \pmod m$ and $x \equiv b \pmod n$ such that $gcd(m, n) = 1$, then $x \equiv c \pmod{mn}$ where $c = bm_n^{-1}m + an_m^{-1}n$ where m_n^{-1} is the inverse of m modulo n and n_m^{-1} is the inverse of n modulo m.

2. (Chicken McNugget Theorem) For any two relatively prime positive integers m, n, the greatest integer that cannot be written in the form $am + bn$ for nonnegative integers a, b is $mn - m - n$.

3. (Lagrange's Theorem) The congruence $f(x) \equiv 0 \pmod p$, where p is prime, and $f(x) = a_0x^n + \cdots + a_n$ is a polynomial with integer coefficients such that $a_0 \not\equiv 0 \pmod p$, has at most n in-congruent roots modulo p.

4. (Primitive Roots Theorem) A primitive root modulo n exists if and only if n is equal to $2, 4, p^k, 2p^k$, where p is an odd prime number and k is a positive integer. If a primitive root modulo n exists, there are exactly $\varphi(\varphi(n))$ of these primitive roots.

5. (Euler's Criterion)

$$a^{\frac{p-1}{2}} \equiv \begin{cases} 1 \pmod p & \iff \text{there is an integer } x \text{ such that } a \equiv x^2 \pmod p \\ -1 \pmod p & \iff \text{there is no such integer.} \end{cases}$$

6. (Dirichlet's Theorem) For any co-prime pairs a, n, there are infinitely many primes that equivalent to $a \pmod n$. A stronger form of this theorem states that the infinite sum of the reciprocals of all primes that are equivalent to $a \pmod n$ is divergent or approaches infinity.

9 Olympiad Problems

In no particular order:

1. (CMO 2011) Consider 70-digit numbers with the property that each of the digits $1, 2, 3, ..., 7$ appear 10 times in the decimal expansion of n (and $8, 9, 0$ do not appear). Show that no number of this form can divide another number of this form.

2. (INMO 2012) Let $p_1 < p_2 < p_3 < p_4$ and $q_1 < q_2 < q_3 < q_4$ be two sets of prime numbers, such that $p_4 - p_1 = 8$ and $q_4 - q_1 = 8$. Suppose $p_1 > 5$ and $q_1 > 5$. Prove that 30 divides $p_1 - q_1$.

3. (USAMO 2017) Prove that there are infinitely many distinct pairs (a, b) of relatively prime positive integers $a > 1$ and $b > 1$ such that $a^b + b^a$ is divisible by $a + b$.

4. (JBMO 2011 Shortlist) Find all positive integer triplets x, y, z such that $1005^x + 2011^y = 1006^z$

5. (USAMO 2018) Let p be a prime, and let $a_1, \ldots, a_p$ be integers. Show that there exists an integer k such that the numbers
$$a_1 + k, a_2 + 2k, \ldots, a_p + pk$$
produce at least $\frac{1}{2}p$ distinct remainders upon division by p.

6. (APMO 2006) Let $p \geq 5$ be a prime and let r be the number of ways of placing p checkers on a p x p checkerboard so that not all checkers are in the same row (but they may all be in the same column). Show that r is divisible by p^5. Here, we assume that all the checkers are identical.

7. (INMO 2018) Let $\mathbb{N}$ denote set of all natural numbers and let $f : \mathbb{N} \to \mathbb{N}$ be a function such that
   - $f(mn) = f(m) \cdot f(n)$ for all $m, n \in \mathbb{N}$
   - $m + n$ divides $f(m) + f(n)$ for all $m, n \in \mathbb{N}$.

   Prove that all functions must be of the form $f(n) = n^k$, where k is an odd integer.

8. (CMO 2009) Find all ordered pairs of integers (a, b) such that $3^a + 7^b$ is a perfect square.

9. (INMO 2015) Show that from a set of 11 square integers one can select six numbers $a^2, b^2, c^2, d^2, e^2, f^2$ such that $a^2 + b^2 + c^2 \equiv d^2 + e^2 + f^2 \pmod{12}$.

10. (Winter Camp Warm-up N2 2019) A prime p and a positive integer n are given. The product $(1^3 + 1)(2^3 + 1) \cdots ((n-1)^3 + 1)(n^3 + 1)$ is divisible by p^3. Prove that $p \leq n + 1$.

11. (APMO 2016) A positive integer is called fancy if it can be expressed in the form
$$2^{a_1} + 2^{a_2} + \cdots + 2^{a_{100}},$$
where $a_1, a_2, \cdots, a_{100}$ are non-negative integers that are not necessarily distinct. Find the smallest positive integer n such that no multiple of n is a fancy number.