Applications of congruences and divisibility: elementary number theory questions

This is a summary and a few examples that we did in class on 9/6.

1. Computing remainders. Use properties of congruences to compute remainders easily.
Example 1.1. Show that 7 divides $3^{2n+1} + 2^{n+2}$ for every $n \geq 1$.

Solution.

$$3^{2n+1} + 2^{n+2} = 3 \cdot 9^n + 4 \cdot 2^n \equiv 3 \cdot 2^n + 4 \cdot 2^n \equiv 7 \cdot 2^n \equiv 0 \mod 7.$$

We used properties of congruences: $9 \equiv 2 \mod 7$ so $9^n \equiv 2^n \equiv 7$.

Example 1.2. Find the last digit of 3^{2023}.

Solution. The last digit of a positive integer n is congruent to $n \mod 10$. To find the remainder of 3^{2023} mod 10, notice that $9 \equiv -1 \mod 10$. In these questions, -1 is always your friend. Then

$$3^{2023} = 3 \cdot 9^{1011} \equiv 3 \cdot (-1)^{1011} \equiv -3 \equiv 7.$$

The last digit is 7.

2. Divisibility criteria. Let a positive integer A be written in decimal notation as

$$A = \overline{a_n a_{n-1} \dots a_2 a_1 a_0}.$$

This notation means that A has n digits, $a_n, \dots, a_1, a_0$, so that

$$A = 10^n \cdot a_n + 10^{n-1} \cdot a_{n-1} + \dots 10^2 \cdot a_2 + 10 \cdot a_1 + a_0.$$

Divisibility by 2 and 5. Obviously, $A \equiv a_0 \mod 2$ and $\mod 5$, since 2 and 5 divide 10. This means that in these cases, divisibility and remainder is determined by the last digit.

Divisibility by 4. Since 4 divides 100, we see that $A \equiv 10a_1 + a_0 \mod 4$. Thus, divisibility by 4 and the remainder are determined by the 2-digit integer formed by the last two digits of A.

Divisibility by 3 and 9. Using the fact that $10 \equiv 1 \mod 9$ and therefore $10^n \equiv 1 \mod 9$, we get that

$$A \equiv a_n + a_{n-1} + \dots + a_2 + a_1 + a_0 \mod 9,$$

that is, the positive integer A is congruent $\mod 9$ to the sum of its digits. The same is true $\mod 3$, since 3 divides 9.

3. Perfect squares. One could wonder whether a given integer a can be a square of another integer, so that $a = n^2$ for some n. If this is the case, a is called a perfect square. Perfect squares have some special properties.

Prime divisors of perfect squares. If $a = n^2$ is divisible by a prime p, then it must be divisible by p^2. This follows from the prime factorization (and its uniqueness!): for a to be divisible by p, n must have a factor of p in its prime factorization, and then a must have p^2.

Remainders of perfect squares. There are some useful congruences for perfect squares:

Remainders of $a = n^2 \mod 3$ and $\mod 4$ can only be 0 and 1.

This is easily checked by considering cases: $n \equiv 0 \mod 3$, $n \equiv 1 \mod 3$, $n \equiv 2 \mod 3$ and squaring these congruences (and similarly checking remainders 0, 1, 2, 3 mod 4).

Example 3.1. Consider the integer $A = 111 \dots 11$ consisting of 100 1's in decimal notation. Is A a perfect square?

Solution. By divisibility criteria, $A \equiv 11 \equiv 3 \mod 4$, but this is not possible for a perfect square. (Note that arguing $\mod 3$ would give no conclusion since $A \equiv 100 \equiv 1 \mod 3$.)

4. Prime and composite numbers. Proving that a given integer is prime is hard (unless you can directly check that it has no non-trivial divisors); to prove that a number is composite, it suffices to find a non-trivial divisor or factorization. You can use the arithmetic of congruences or divisibility criteria to find divisors: for example, $3^{2n+1} + 2^{n+2}$ is divisible by 7 for every $n \geq 1$ by Example 1.1, and since it is greater than 7, it cannot be prime. Another method is to use algebra to find a factorization. Formulas for differences of squares and cubes and sums of cubes are useful. The following two formulas generalize them:

$$a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + a^{n-3}b^2 + \cdots + ab^{n-2} + b^{n-1}), \quad n \geq 1,$$

$$a^n + b^n = (a+b)(a^{n-1} - a^{n-2}b + a^{n-3}b^2 \pm \cdots - ab^{n-2} + b^{n-1}), \quad n \geq 1, \quad n \text{ odd}.$$

Both formulas can be easily proved by multiplying out: most terms will cancel.

Example 4.1. Prove that $2^n + 1$ cannot be prime unless n is a power of 2.

Solution. If n is not a power of 2, the prime decomposition tells us that n must have an odd divisor $m > 1$, so that $n = m \cdot k$ for some integer k. (We might have $n = m$, $k = 1$, but we always get $k < n$ since $m > 1$.) Then we have

$$2^n + 1 = (2^k)^m + 1 = (2^k + 1)((2^k)^{m-1} - (2^k)^{m-2} \pm \cdots + 1)$$

by the formula for the sum of mth powers, m odd. We need to check that the factorization is nontrivial: we have $2^k + 1 \geq 3 > 1$ and $2^k + 1 < 2^n + 1$. So the factorization shows that $2^n + 1$ is composite.