Congruence

Section 1. Basic Concepts.

When divided by a positive integer m, if both the integers a and b leave the same remainder, then they are said to be **congruent** to each other **modulo** m. This is denoted by $a \equiv b \pmod{m}$. For example, since $20 = 7 \times 2 = 6$ and $-8 = 7 \times (-2) + 6$, 20 and -8 both leave the remainder 6 when divided by 7. Hence they are congruent to each other modulo 7. We write $20 \equiv -8 \pmod{7}$.

The concept of congruent numbers is called **congruence**. It is a **binary relation**, that is, a relation between two numbers. Other examples of binary relations are $<$, $\geq$ and $=$. Congruence has the following three properties. Let m be a given positive integer.

(1) **Reflexive Property**.
Every integer is congruent to itself modulo m. In other words, $a \equiv a \pmod{m}$ for every integer a.

(2) **Symmetric Property.**
If an integer a is congruent modulo m to another integer b, then b is congruent to a. In other words, if $a \equiv b \pmod{m}$, then $b \equiv a \pmod{m}$.

(3) **Transitive Property.**
If an integer a is congruent modulo m to another integer b, and b is congruent modulo m to a third integer c, then a is congruent modulo m to c. In other words, if $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$.

A binary relation with all these properties is called an **equivalence relation**. It partitions the overall structure into disjoint classes so that elements in the same class are related to one another, and two different elements in different classes are not related to each other. These classes are called **equivalence classes**.

For a given positive integer m, congruence modulo m partitions the integers into m equivalence classes, according to their remainders when divided by m. Thus congruence modulo 2 partitions the integers into odd and even numbers. Congruence modulo 10 partitions the integers according to their units digits.

Like equations, congruences can be added and multiplied. Suppose $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$. This means that when divided by m, both a and b leave the same reaminder r and both c and d leave the same remainder s. Now $0 \leq r < m$ and $0 \leq s < m$. Hence $0 \leq r + s < 2m$. If $r + s < m$, then it is the remainder when both $a + c$ and $b + d$ are divided by m. If $m \leq r + s < 2m$, then $0 \leq r + s - m < m$, and $r + s - m$ is the remainder when both $a + c$ and $b + d$ are divided by m. In either case, we have $a + c \equiv b + d \pmod{m}$. Another way of saying this is $a + c \equiv r + s \equiv b + d \pmod{m}$. Now $a = qm + r$ and $c = pm + s$ for some positive integers q and p. Hence $ac = (qm + r)(pm + s) = m(pqm + pr + qs) + rs$. Hence $ac \equiv rs \pmod{m}$. Similarly, $bd \equiv rs \pmod{m}$. Hence $ac \equiv bd \pmod{m}$.

For example, we have $20 \equiv -8 \pmod{7}$ and $33 \equiv 5 \pmod{7}$. Then $53 \equiv 20 + 33 \equiv -8 + 5 = -3 \pmod{7}$ and $660 = 20 \times 33 \equiv -8 \times 5 = -40 \pmod{7}$. Indeed $53 = 7 \times 7 + 4$, $-3 = 7 \times (-1) + 4$, $660 = 74 \times 7 + 2$ and $-40 = 7 \times (-6) + 2$.

Section 2. Some Simple Appications.

Congruence modulo 3 partitions the integers into the following three classes:

$$\begin{array}{ccccccccccccccc}
\cdots & -9 & -6 & -3 & \mathbf{0} & 3 & 6 & \mathbf{9} & 12 & 15 & 18 & 21 & 24 & 27 & \cdots \\
\cdots & -8 & -5 & -2 & \mathbf{1} & \mathbf{4} & 7 & 10 & 13 & \mathbf{16} & 19 & 22 & \mathbf{25} & 28 & \cdots \\
\cdots & -7 & -4 & -1 & 2 & 5 & 8 & 11 & 14 & 17 & 20 & 23 & 26 & 29 & \cdots
\end{array}$$

The boldfaced entries are the squares. So far, that they all appear in the first two classes. This is in fact always the case. Consider where the square of an integer a would appear. When a is divided by 3, the remainders must be one of 0, 1 and 2, so that $a \equiv 0 \pmod 3$, $a \equiv 1 \pmod 3$ or $a \equiv 2 \pmod 3$. If $a \equiv 0 \pmod 3$, then $a^2 \equiv 0^2 = 0 \pmod 3$. If $a \equiv 1 \pmod 3$, then $a^2 \equiv 1^2 = 1 \pmod 3$. If $a \equiv 2 \pmod 3$, then $a^2 \equiv 2^2 = 4 \equiv 1 \pmod 3$. It follows that a^2 is never congruent to 2 modulo 3.

We can prove a similar result for congruence modulo 4. If $a \equiv 0 \pmod 4$, then $a^2 \equiv 0^2 = 0 \pmod 4$. If $a \equiv 1 \pmod 4$, then $a^2 \equiv 1^2 = 1 \pmod 4$. If $a \equiv 2 \pmod 4$, then $a^2 \equiv 2^2 = 4 \equiv 0 \pmod 4$. If $a \equiv 3 \pmod 4$, $a^2 \equiv 3^3 = 9 \equiv 1 \pmod 4$. It follows that a^2 is never congruent to 2 or 3 modulo 4. This idea can be applied to a^k and modulo m for other values of k and m.

Note that $10 \equiv 1 \pmod 9$. It follows that $10^k \equiv 1 \pmod 9$ for any positive integer k. This allows us to find the remainder in a division by 9 without performing the actual division itself. Consider the following example.

$$\begin{aligned}
7804132211 &= 7 \times 10^9 + 8 \times 10^8 + 0 \times 10^7 + 4 \times 10^6 + 1 \times 10^5 + 3 \times 10^4 \\
&\quad + 2 \times 10^3 + 2 \times 10^2 + 1 \times 10 + 1 \\
&= 7 + 8 + 0 + 4 + 1 + 3 + 2 + 2 + 1 + 1.
\end{aligned}$$

Since $7 + 8 + 0 + 4 + 1 + 3 + 2 + 2 + 1 + 1 = 29 \equiv 1 \pmod 9$, the remainder when 7804132211 is divided by 9 is 1. In general, every positive integer is congruent modulo 9 to the sum of its digits. This is the basis of the test of divisibility by 9, in that a positive integer is divisible by 9 if and only if the sum of its digits is divisible by 9. We also get a true statement if we replace 9 by 3.

On the other hand, $10 \equiv -1 \pmod{11}$. It follows that $10^k \equiv 1 \pmod{11}$ for any even positive integer k and $10^k \equiv -1 \pmod{11}$ for any odd positive integer k.

$$\begin{aligned}
7804132211 &= 7 \times 10^9 + 8 \times 10^8 + 0 \times 10^7 + 4 \times 10^6 + 1 \times 10^5 + 3 \times 10^4 \\
&\quad + 2 \times 10^3 + 2 \times 10^2 + 1 \times 10 + 1 \\
&= -7 + 8 - 0 + 4 - 1 + 3 - 2 + 2 - 1 + 1.
\end{aligned}$$

Since $-7 + 8 - 0 + 4 - 1 + 3 - 2 + 2 - 1 + 1 = 7 \pmod{11}$, the remainder when 7804132211 is divided by 11 is 7. In general, every positive integer is congruent modulo 11 to the alternate sum of its digits, with the units digit being positive. This is the basis of the test of divisibility by 11, in that a positive integer is divisible by 11 if and only if the alternate sum of its digits is divisible by 11.

Section 3. Contest Problems.

Below are several related problems on the 2014-digit number n consisting of all 9s except for a 1 as its last digit.

Problem 1.
Prove that n is a composite number.

Problem 2.
Prove that n is not a square.

Problem 2 is needed to set up the next problem. A positive integer which is not a square has an even number of positive divisors because they form pairs whose product is n. If n is a square, which means that $\sqrt{n}$ is a positive integer, then it is paired with itself. It counts as only one divisor, making the total number of divisors odd. By Problem 2, n has $2k$ positive divisors for some positive integer k, namely, $1 = d_1 < d_2 < \cdots < d_k < d_{k+1} < \cdots < d_{2k-1} < d_{2k} = n$.

Problem 3.
Find the combined digit sum of d_k and d_{k+1}.

Problem 4.
Find the combined digit sum of d_2 and d_{2k-1}.

Problem 1 was proposed for a junior high school mathematics contest. Since numerical answers were desired, it was intended to be modified as Problem 3. However, the problem was worded so that Problem 4 became what was actually asked.

Solution to Problem 1.
Note that $n = 10^{2014} - 9 = (10^{1007})^2 - 3^2 = (10^{1007} + 3)(10^{1007} - 3)$. Since each factor is clearly greater than 1, n is a composite number.

Solution to Problem 2.
Note that $n = 999\ldots991 = 999\ldots9 \times 100 + 91 \equiv 0 + 3 = 3 \pmod 4$ since $100 \equiv 0 \pmod 4$. Since all squares are congruent to 0 or 1 (mod 4), n is not a square.

Solution to Problem 3.
Note that $d_k = 10^{1007} - 3 = 999\ldots997$ so that its digit sum is $1006 \times 9 + 7 = 9061$. On the other hand, $d_{k+1} = 1000\ldots003$ so that its digit sum is 1+3=4. Hence the combined digit sum is 9061+4=9065.

The rest of the article is devoted to the solution to Problem 4.

Clearly, $d_2 \neq 2$ or 5. By the tests of divisibility, it is neither 3 nor 11. If $d_2 = 7$, then we must have $10^{2014} \equiv 9 \equiv 2 \pmod 7$. Now $10 \equiv 3 \pmod 7$, $10^2 \equiv 3 \times 3 = 9 \pmod 7$, $10^3 \equiv 3 \times 9 = 27 \equiv 6 \pmod 7$, $10^4 \equiv 3 \times 6 = 18 \equiv 4 \pmod 7$, $10^5 \equiv 3 \times 4 = 12 \equiv 5 \pmod 7$ and $10^6 \equiv 3 \times 5 = 15 \equiv 1 \pmod 7$. It is not necessary to go on any further. This is because $2014 = 335 \times 6 + 4$, so that $10^{2014} = (10^6)^{335} \times 10^4 \equiv 1^{335} \times 4 = 4 \neq 2$. It follows that $d_2 \neq 7$.

A key step in the above argument is that $10^k \equiv 1 \pmod 7$ for some positive integer k, which happens to be 6. How do we know that such a k always exists, if we replace 7 by another prime number? Let us understand why $k = 6$ for the prime number 7. Suppose we wish to convert the fraction $\frac{1}{7}$ into a decimal. By long division, we find that $\frac{1}{7} = 0.\overline{142857}$, a decimal expansion consisting of repeating blocks of the six digits 142857.

The reason that there are six digits is that when we divide by 7, the only possible remainders are 0, 1, 2, 3, 4, 5 and 6. Here 0 will not appear since no power of 10 is divisible by 7. By the time we have seen each of the non-zero remainders once, repetition must start. Thus the repeating block of decimal digits has length at most 6. In this case, it happends to be exactly 6. This means that $\frac{1}{7} = \frac{142857}{999999}$ so that 999999 is divisible by 7. It follows that $10^6 \equiv 1$.

In a similar manner, we can prove that $d_2 \neq 13$, 17, 19 or 23. We know that $10^{12} \equiv 1 \pmod{13}$, $10^{16} \equiv 1 \pmod{17}$, $10^{18} \equiv 1 \pmod{19}$ and $10^{22} \equiv 1 \pmod{23}$. As it turns out, $10^6 \equiv 1 \pmod{13}$, but the other powers, namely, 16, 18 and 22, cannot be reduced. Since $10^4 \not\equiv 9 \pmod{13}$, $d_2 \neq 13$. Now $2014 = 125 \times 16 + 14$ but $10^{14} \not\equiv 9 \pmod{17}$, $2014 = 111 \times 18 + 16$ but $10^{16} \not\equiv 9 \pmod{19}$, and $2014 = 91 \times 22 + 12$ but $10^{12} \not\equiv 9 \pmod{23}$. Hence $d_2 \neq 17$, 19 or 23.

The next candidate for d_2 is 29. We know that $10^{28} \equiv 1$, but perhaps one of 10^2, 10^4, 10^7 and 10^{14} may be too. In modulo 29, we have $10^2 = 100 \equiv 13$, $10^3 \equiv 10 \times 13 = 130 \equiv 14$, $10^4 \equiv 10 \times 14 = 140 \equiv 24$, $10^7 \equiv 14 \times 24 = 336 \equiv 17$ and $10^{14} \equiv 17^2 = 289 \equiv 28$. So this does not happen. Since $2014 = 28 \times 71 + 26$, what we need is $10^{26} \equiv 9$ Now $10^5 \equiv 24 \times 10 = 240 \equiv 8$, $10^{25} \equiv 8^5 = 32768 \equiv 27$ and $10^{26} \equiv 10 \times 27 = 270 \equiv 9$. This is exactly what we want.

We are lucky that $n = 10^{2014} - 9 = (10^{1007} + 3)(10^{1007} - 3)$ has a prime factor as small as 29. Each of $10^{1007} + 3$ and $10^{1007} - 3$ has more than 1000 digits. Even if they were not prime numbers, they could have been products of prime numbers with over 500 digits. It would be very difficult to find d_2 then.

From $d_2 = 29$, we have $d_{2k-1} = \frac{n}{29}$. There remains only the trivial matter of determining their combined digit sums, via the following long division.

```
                 344827   5862068   9655172   4137931
          ------------------------------------------
29 )9999999   9999999   9999999   9999999
   9999983
   ---------
        16   9999999
        16   9999972
   ---------------------
                 27   9999999
                 27   9999988
   ---------------------------
                          11   9999999
                          11   9999999
   ---------------------------------
```

The sum of the digits of the quotient is 126, and there are 71 such blocks. In the last incomplete block, the quotient is without the last two digits 3 and 1. It follows that the digit sum of d_{2k-1} is $126 \times 71 + 122 = 9068$. Since the digit sum of d_2 is 11, the combined digit sum is 9079.

The solution of the following two problems are left to the readers.

Problem 5.

Determine which of $10^{1007} + 3$ and $10^{1007} - 3$ is divisible by 29.

Problem 6.

For what year $y > 2014$ would the second smallest positive divisor of $10^y - 9$ be
(a) 7; (b) 13; (c) 17; (d) 19; (e) 23?