DIS 4B

1 Amaze Your Friends

You want to trick your friends into thinking you can perform mental arithmetic with very large numbers. What are the last digits of the following numbers?

(a) 11^{2017}

(b) 9^{10001}

(c) $3^{987654321}$

Solution:

(a) 11 is always 1 mod 10, so the answer to (a) is 1.

(b) 9 is its own inverse mod 10, therefore, if 9 is raised to an odd power, the number will be 9 mod 10. So the answer is 9.

Also notice that $9 \equiv -1 \pmod{10}$ so $9^{10001} \equiv (-1)^{10001} \equiv -1 \equiv 9 \pmod{10}$. In general, $m-1 \equiv -1 \pmod{m}$, so $m-1$ is always its own inverse. This is a useful trick so you can avoid computing the inverse of $m-1$ by hand. You can also check that $(m-1)^2 \equiv m^2 - 2m + 1 \equiv 1 \pmod{m}$, which is another proof that $m-1$ is its own inverse modulo m.

(c) $3^4 = 9^2 = 1$ mod 10. We see that the exponent $987654321 = 1$ mod 4 so the answer is 3.

2 Combining Moduli

Suppose we wish to work modulo $n = 40$. Note that $40 = 5 \times 8$, with $\gcd(5,8) = 1$. We will show that in many ways working modulo 40 is the same as working modulo 5 and modulo 8, in the sense that instead of writing down $c \pmod{40}$, we can just write down $c \pmod{5}$ and $c \pmod{8}$.

(a) What is $8 \pmod{5}$ and $8 \pmod{8}$? Find a number $a \pmod{40}$ such that $a \equiv 1 \pmod{5}$ and $a \equiv 0 \pmod{8}$.

(b) Now find a number $b \pmod{40}$ such that $b \equiv 0 \pmod{5}$ and $b \equiv 1 \pmod{8}$.

(c) Now suppose you wish to find a number $c \pmod{40}$ such that $c \equiv 2 \pmod{5}$ and $c \equiv 5 \pmod{8}$. Find c by expressing it in terms of a and b.

(d) Repeat to find a number $d \pmod{40}$ such that $d \equiv 3 \pmod{5}$ and $d \equiv 4 \pmod{8}$.

(e) Compute $c \times d \pmod{40}$. Is it true that $c \times d \equiv 2 \times 3 \pmod{5}$, and $c \times d \equiv 5 \times 4 \pmod{8}$?

Solution:

(a) $8 \equiv 3 \pmod{5}$ and $8 \equiv 0 \pmod{8}$. We can find such a number by considering multiples of 8, i.e. 0, 8, 16, 24, 32, and find that if $a = 16$, $16 \equiv 1 \pmod{5}$. Therefore 16 satisfies both conditions.

(b) We can find such a number by considering multiples of 5, i.e. 0, 5, 10, 15, 20, 25, 30, 35, and find that if $b = 25$, $25 \equiv 1 \pmod{8}$, so it satisfies both conditions.

(c) We claim $c \equiv 2a + 5b \equiv 37 \pmod{40}$. To see that $c \equiv 2 \pmod{5}$, we note that $b \equiv 0 \pmod{5}$ and $a \equiv 1 \pmod{5}$. So $c \equiv 2a \equiv 2 \pmod{5}$. Similarly $c \equiv 5b \equiv 5 \pmod{8}$.

(d) We can repeat the same procedure as above, and find that $d = 3a + 4b \equiv 28 \pmod{40}$.

(e) $c \times d = 37 \times 28 \equiv 36 \pmod{40}$. Note that if $w \equiv x \pmod{n}$ and $y \equiv z \pmod{n}$ then $w \times y \equiv x \times z \pmod{n}$. Therefore we can multiply $c \equiv 2 \pmod{5}$ and $d \equiv 3 \pmod{5}$ to get $c \times d \equiv 2 \times 3 \pmod{5}$. Similarly we can multiply these equations modulo 8 and get $c \times d = 5 \times 4 \pmod{8}$.

3 Baby Fermat

Assume that a does have a multiplicative inverse mod m. Let us prove that its multiplicative inverse can be written as $a^k \pmod{m}$ for some $k \geq 0$.

(a) Consider the sequence $a, a^2, a^3, \ldots \pmod{m}$. Prove that this sequence has repetitions.

(b) Assuming that $a^i \equiv a^j \pmod{m}$, where $i > j$, what can you say about $a^{i-j} \pmod{m}$?

(c) Prove that the multiplicative inverse can be written as $a^k \pmod{m}$. What is k in terms of i and j?

Solution:

(a) There are only m possible values mod m, and so after the m-th term we should see repetitions.

(b) We will temporarily use the notation a^* for the multiplicative inverse of a to avoid confusion. If we multiply both sides by $(a^*)^j$ in the third line below, we get

$$\begin{aligned}
a^i &\equiv a^j && \pmod{m}, \\
a^{i-j}\underbrace{a\cdots a}_{j\text{ times}} &\equiv \underbrace{a\cdots a}_{j\text{ times}} && \pmod{m}, \\
a^{i-j}\underbrace{a\cdots a}_{j\text{ times}}\cdot\underbrace{a^*\cdots a^*}_{j\text{ times}} &\equiv \underbrace{a\cdots a}_{j\text{ times}}\cdot\underbrace{a^*\cdots a^*}_{j\text{ times}} && \pmod{m}, \\
a^{i-j} &\equiv 1 && \pmod{m}.
\end{aligned}$$

(c) We can rewrite $a^{i-j} \equiv 1 \pmod{m}$ as $a^{i-j-1}a \equiv 1 \pmod{m}$. Therefore a^{i-j-1} is the multiplicative inverse of $a \pmod{m}$.