Iowa City Math Circle Handouts

June 23, 2019

3 Modular Arithmetic and Bases

3.1 Warm-up Problems

Remember: Use modular arithmetic!

1. Find the remainder when $1 + 8 + 15 + 22 + \cdots + 701$ is divided by 7.
2. Find the remainder when 19^{19} is divided by 5.
3. x, y, and z are positive integers so that $x \equiv 1 \pmod 9$, $y \equiv 2 \pmod 9$, and $z \equiv 3 \pmod 9$. What is the remainder when the product xyz is divided by 9?

3.2 Bases

The number system we use in everyday life is called *base-10*. This is because each digit represents a quantity of powers of 10. For example, the number $1234 = 1 \cdot 10^3 + 2 \cdot 10^2 + 3 \cdot 10^1 + 4 \cdot 10^0$.

In the same way, we can also express numbers in different bases. For example, 432 in base 6 (denoted by 432_6) would be equivalent to $4 \cdot 6^2 + 3 \cdot 6^1 + 2 \cdot 6^0 = 164$ in base 10.

Numbers are different bases are usually denoted with a subscript that indicates their base; for example, 432_6.

How can we convert numbers to different bases? We can use a process like division.

Example 4. *Convert* 100_{10} *to base 3.*

Solution. The highest power of 3 that is less than 100 is $3^4 = 81$. $100/81 = 1$ with a remainder of 19, so the digit in the 3^4 place will be 1:

$$1\_\_\_\_$$

Since $3^3 = 27$ is greater than 19, we have a 0 in the 3^3 place:

$$10\_\_\_$$

The next highest power of 2 that is less than 19 is 9. $19/9 = 2$ with a remainder of 1, so we have 2 in the 3^2 place:

$$102\_\_$$

$3^1 > 1$, so there is a 0 in 3^1 place:

$$1020\_$$

Since we have a 1 left over, we have a 1 in the 3^0 place:

$$\boxed{10201}$$

△

All base 10 operations such as addition, multiplication, subtraction, and division also work in different bases. However, operations like "carrying" must be done in the given base. A common metaphor for this is doing arithmetic "on a clock."

Example 5. *Add* 432_6 *and* 234_6. *Give the result in base 6.*

Solution.
$$\begin{array}{r} 1\,1 \\ 4\,3\,2 \\ +2\,3\,4 \\ \hline 1\,1\,1\,0 \end{array}$$

Notice that we have a carry in the first column of addition $(2+4)$ because $(2+4=6=1\cdot 6)$. Hence, the last digit is 0. For the addition in the second column, $1+3+3=7=1\cdot 6+1$, so the third digit is 1 and the carry to the third column is 1. For the addition in the third column, $1+2+4=7=1\cdot 6+1$, so the second digit is 1 and the first digit is 1. △

One of the commonly tested concepts in math competitions regarding bases is base conversion. To convert a number from one base to another, first convert that number to base 10 and then convert this base 10 number to the desired base.

However, there are some clever short cuts for specific bases. For example, if you want to convert a base 2 number to base 8, you add zeros to the front of the number to make the number of digits a multiple of 3 and you make groups of 3 digits starting from the right. Then, you synthesize each group into a base 10 numeral by treating each group as a 3-digit numeral in base 2. Next, convert these base-10 numbers to base-8. Finally, group all these base 8 numbers in the original order to get the final answer in base 8.

Example 6. *Convert* 1101010101_2 *to base 8.*

Solution. We make the groups 101, 010, 101, and 001. Then, we have $101_2=5_8$, $010_2=2_8$, $101_2=5_8$, and $001_2=1_8$. Hence, $1101010101_2=\boxed{1525_8}$. △

This method can be easily generalized for converting a base n numeral to base n^k, where k is a positive integer (i.e. n^k is a power of n) and can be reversed to convert a base n^k numeral to n.

3.2.1 Review Exercises

1. Convert the binary number 111010_2 to base 4, both manually and then by using the shortcut described above (Example 6).

3.3 Modular Inverses

Every integer relatively prime to m has a *modular inverse* in mod m. This means that if a^{-1} is the modular inverse of $a \pmod{m}$, where $\gcd(a,m)=1$, then $a\cdot a^{-1}\equiv 1 \pmod{m}$. The modular inverse of $a \pmod{m}$ is always such that $1\le a^{-1}\le m-1$ (so you only have to check these numbers).

Example 7. *Find the modular inverse of 2 in mod 7.*

Solution. Notice that $2 \cdot 4 \equiv 8 \equiv 1 \pmod 7$. Thus the modular inverse of $2 \mod 7$ is $\boxed{4}$. △

Note that it is also possible for a number's modular inverse to be itself.

3.3.1 Review Exercises

1. Find the modular inverse of $3 \pmod 8$.
2. Compute 997^{-1} modulo 1000. Express your answer as an integer from 0 to 999.

3.4 Euler's Totient Function

The totient function applies to all positive integers, and returns the number of integers coprime to n which are less than n. The totient function is denoted ϕ.

Example 8. *Calculate* $\phi(6)$

Solution. To calculate $\phi(6)$, we must find the number of integers less than 6 such that $\gcd(m, 6) = 1$. To do this, we can simply run through the integers 1 through 5.

$$\begin{gathered}\gcd(1,6) = 1\\ \gcd(2,6) = 2\\ \gcd(3,6) = 3\\ \gcd(4,6) = 2\\ \gcd(5,6) = 1\end{gathered}$$

So only 1 and 5 are relatively prime to 6, so $\phi(6) = \boxed{2}$ △

However, instead of checking all the integers 1 to $n - 1$, we can use the following formula:

$$\phi(n) = \prod_{i=1}^{k}(p_i^{a_i} - p_i^{a_i-1}) = (p_1^{a_1} - p_1^{a_1-1}) \cdot (p_2^{a_2} - p_2^{a_2-1}) \ldots (p_k^{a_k} - p_k^{a_k-1})$$

where the prime factorization of n is $p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k}$

Example 9. *Calculate* $\phi(12)$*, first manually (by checking* 1 *through* 11*), and then by using the formula above.*

Solution. First, we must prime factorize 12. $12 = 4 \cdot 3 = 2^2 \cdot 3$. Using the formula above, we get

$$\phi(12) = (2^2 - 2^1) \cdot (3^1 - 3^0) = \boxed{4}$$

△

Example 10. *Find a general formula for* $\phi(p)$*, where* p *is a prime.*

Solution. First, to use the formula above, we must find the prime factorization of p. However, since p is prime, the prime factorization is just p. Plugging this into the formula, we get

$$\phi(p) = (p^1 - p^0) = \boxed{p-1}$$

△

3.4.1 Review Exercises

1. Calculate $\phi(15)$.
2. Find $\phi(10^n)$ in terms of n, where n is any positive integer.

3.5 Euler's Theorem

Euler's Theorem: $a^{\phi(n)} \equiv 1 \mod n$, where $\gcd(a, n) = 1$.

Fermat's Little Theorem: $a^{p-1} \equiv 1 \pmod p$, where p is a prime and $\gcd(a, p) = 1$.

Example 11. *Calculate the remainder when* 9^{42} *is divided by* 100.

Solution. To rephrase the problem in terms of modular arithmetic, we must calculate $9^{42} \mod 100$. To use Euler's Theorem, we first must check that $\gcd(9, 100)$ is 1, which is true. (Don't forget this step!) Next, we will calculate $\phi(100) = (2^2 - 2^1) \cdot (5^2 - 5^1) = 40$. Hence, $9^{40} \equiv 1 \mod 100$. This is not exactly what we want; we must end up with 9^{42} on the left. So we can multiply both sides by 9^2, to get $9^{42} \equiv 9^2 \mod 100$. So our answer is $9^2 = \boxed{81}$. △

3.5.1 Review Exercises

1. Show Fermat's Little Theorem using Euler's Theorem, using the result from Example 10.

3.6 Problems

Starred exercises are challenge problems.

1. Each pack of hot dogs contains 10 hot dogs (no buns), but each pack of hot dog buns contains 8 buns. Phil buys a number of these packs for a barbecue. After the barbecue, Phil finds that he has 4 hot dogs left over. What is the SECOND smallest number of packs of hot dogs he could have bought? *Source: Alcumus*
2. What is the smallest positive multiple of 23 that is 4 more than a multiple of 89? *Source: Alcumus*
3. You have seven bags of gold coins. Each bag has the same number of gold coins. One day, you find a bag of 53 coins. You decide to redistribute the number of coins you have so that all eight bags you hold have the same number of coins.

You successfully manage to redistribute all the coins, and you also note that you have more than 200 coins. What is the smallest number of coins you could have had before finding the bag of 53 coins? *Source: Alcumus*

4. What is the last digit of $((((7)^7)^7)^{\cdots})^7$ if there are 1000 7s as exponents and only one 7 in the middle? *Source: AoPS*

5. Let S be a subset of $\{1, 2, 3, ..., 50\}$ such that no pair of distinct elements in S has a sum divisible by 7. What is the maximum number of elements in S? *Source: 1992 AHSME Problem 23*

6. * What is the **hundreds** digit of 2011^{2011}? (Hint: Try using Euler's Theorem, then the Binomial Theorem) *Source: 2011 AMC 10B Problem 23*

7. * 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*. *Source: 2014 AIME 1 Problem 8*

Contributors: Daniel Stewart, Ananth Shyamal, Divya Shyamal, Kevin Yang, Reece Yang
iowacitymathcircle.org