#27: Number Theory, Part II: Modular Arithmetic and Cryptography

May 1, 2009

This week you will study *modular arithmetic*—arithmetic where we make the natural numbers "wrap around" by only considering their remainder when divided by some particular number. Modular arithmetic is a foundational subject in number theory, but as we will see, it also has interesting practical applications—for example, it finds many uses in cryptography (the study and design of secret codes).

1 Wrap-around numbers

Modular arithmetic is all about *remainders*. When using modular arithmetic, we pick some particular number n (often, but not always, a prime) called the *modulus*, and say that we are working "modulo n"—this means that we only care about *remainder when dividing by n*.

For example, 12 and 17 are *equivalent modulo* 5 since they have the same remainder (namely, 2) when divided by 5. In this case we write

$$12 \equiv 17 \pmod 5.$$

In other words, when working modulo 5, we put on our "modulo 5 glasses" and 12 and 17 look the same to us. Modulo 5, there are really only five numbers we care about: 0, 1, 2, 3, and 4. After that, the naturals "wrap around" and the pattern repeats: 5 has a remainder of 0 when divided by 5; 6 has a remainder of 1, and so on. Every natural number is equivalent, modulo 5, to some number from 0 to 4.

(You can create modular equivalences in LaTeX with `\equiv` and `\pmod`. For example, the equation above was typeset with `12 \equiv 17 \pmod{5}`.)

Problem 1. State whether each modular equivalence is true or false. For those which are false, give the largest possible modulus which makes the equivalence true. For example, $4 \equiv 7 \pmod 5$ is false, but $4 \equiv 7 \pmod 3$ is true. ($4 \equiv 7 \pmod 1$ is also true, but 1 is not the *largest possible* modulus that works.)

(a) $19 \equiv 23 \pmod 4$

(b) $222 \equiv 23 \pmod{10}$

(c) $30 \equiv 280 \pmod{25}$

(d) $9 \equiv 400 \pmod 2$

Problem 2. Write down four natural numbers that are all equivalent modulo 17.

Problem 3. Can you find five distinct natural numbers so that no two of them are equivalent modulo 4? If so, write down the five numbers; if not, explain why.

Problem 4. Explain how you can tell, just by looking at two numbers, whether they are equivalent modulo 10.

2 Modular arithmetic

When working modulo n, it is as if we have taken the usual number line, like in Figure 1, and wrapped it around to make a circle, like the one in Figure 2.

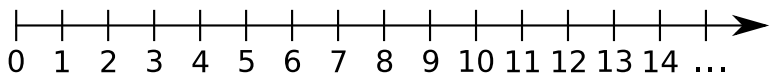

Figure 1: The natural number line

So we can count things, do arithmetic, and so on with the circular number line just like we would with the normal number line—the only difference is that everything above $n - 1$ wraps back around (if we are working modulo n).

Problem 5. Compute each of the following.

(a) $(3 + 5) \bmod 7$

(b) $(4 \times 7 + 6) \bmod 19$

(c) $(1 - 3) \bmod 5$

(d) $(1000!) \bmod 7$

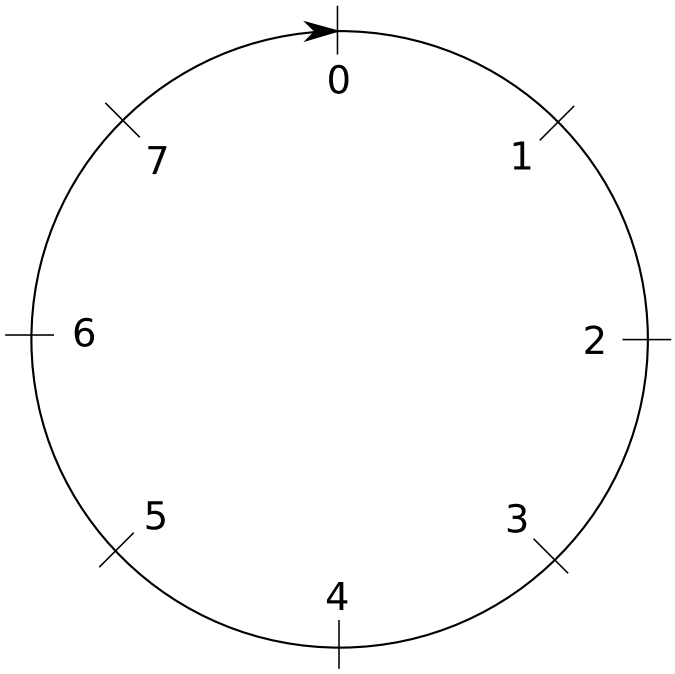

Figure 2: The number line modulo 8

Problem 6. There are quite a few tricks one can use to make things simpler when doing modular arithmetic. Here's one.

(a) Compute $(3^i \bmod 10)$ for $i = 0, 1, 2, 3, 4, 5$.

(b) Do you notice a pattern? Do you think the pattern will continue?

(c) Compute $3^{1247} \bmod 10$.

3 Cæsar ciphers

The *Cæsar cipher* is one of the earliest and most simple forms of cipher. It is named after Julius Cæsar[1], who used it to encrypt messages to his generals. To encrypt a message using a Cæsar cipher, the first step is to convert the letters in the message to numbers from 0 to 25: A is 0, B is 1, and so on. So the message PHISH PHRIEZ would become

15 7 8 18 7 15 7 17 8 4 25.

Next, add some specified amount to each number. For example, let's add 3. However, the key point is that we do this addition *modulo* 26: any numbers larger than 25 wrap back around starting with 0. Performing this operation, we get

18 10 11 21 10 18 10 20 11 7 2.

Note how the 25 wrapped around: $25 + 3 \equiv 2 \pmod{26}$. Finally, we convert back to letters: SKLVK SKULHC would be our encrypted message. The recipient of the message, of course, simply has to reverse the process, assuming that they know the secret number (3, in this example): they just convert the letters to numbers, subtract 3 modulo 26 (which is the same as adding 23) and convert back to letters to read the secret message.

In practice, converting to numbers is unnecessary; it is easy to "count letters" in your head. For example, to add 3 to P, you can just think "P... Q, R, S".

Problem 7. You have intercepted the following encrypted message to your mailman, who you suspect is actually an evil robot from the planet Zorkotron. What should you do?

[1] I'm just using æ because it looks really cool. æ æ æ.

USVV KVV REWKXC IYE KBO YEB YXVI BOWKSXSXQ RYZO
BOWOWLOB SP IYE ROKB DRO GYBN ZKBKUOOD SD GSVV
MKECO IYE DY COVP-NOCDBEMD CY NY XYD CKI SD

4 Vigenère ciphers

As you discovered for yourself in the previous section, a Cæsar cipher is not very secure: there are only 26 possible secret numbers (actually, 25, since 0 is not a very interesting secret number!), and it is entirely feasible to just try them all.

The *Vigenère cipher*, originally invented by Giovan Battista Bellaso (but later misattributed to Blaise de Vigenère), is similar to the Cæsar cipher, but uses a secret *word* (or phrase) instead of a secret *number*. The secret word is often called the "keyword". Intuitively, a Vigenère cipher is much more secure, since it is much harder to guess a secret word than it is to guess a secret number: there are only 25 possible secret numbers, but there are infinitely many possible secret words!

Here's how it works. In a Cæsar cipher, you add the same amount to every letter of the message; in a Vigenère, you add different amounts to different letters, as determined by the secret word. Let's suppose the secret word is PHISH, and we want to encrypt the message DO NOT EAT THE MONKEY. We first line up the secret word underneath the message, repeating it as many times as necessary:

```
D O  N O T  E A T  T H E  M O N K E Y
P H  I S H  P H I  S H P  H I S H P H
```

Now, "add" each letter of the message to the corresponding keyword letter with addition modulo 26, remembering that A corresponds to 0 and Z to 25. For example, D + P = S, since $3 + 15 = 18$; as another example, O + S = G, since $14 + 18 \equiv 6 \pmod{26}$.

```
  D O  N O T  E A T  T H E  M O N K E Y
+ P H  I S H  P H I  S H P  H I S H P H
-----------------------------------------
  S V  V G A  T H B  L O T  T W F R T F
```

So the secret message is SVVGATHBLOTTWFRTF (we often omit the spaces from encrypted messages this way; leaving them in just gives more information to anyone trying to break the encryption, and if you know the secret

word it is not hard to figure out where the spaces go once you have decrypted the message).

Problem 8. Your evil mail-robot (who you destroyed) was carrying a suspicious-looking piece of mail with the following encrypted message:

MTKMQFBMERKVGVHTUCNSWFDINKJ
XPBDIAHXNIYBJFXEIYWWGTNSJQZ

The word "apricot" is written next to it. What should you do?

Problem 9. Although Vigenère ciphers are certainly more secure than Cæsar ciphers, they are not unbreakable. Your answer to this problem should be a message encrypted using a Vigenère cipher. I will attempt to decrypt the message *without* knowing the secret word. If I cannot decrypt it, you will get an automatic score of 5 on this assignment, no matter what you turn in for the other problems. In fact, if you are feeling particularly ambitious, you could just send me a code and not do any of the other problems, and hope I can't solve it—but I don't recommend it. ☺

There are a few requirements:

1. The encrypted message must contain at least 100 letters.
2. The original message must be written in English, using complete sentences and correct grammar and spelling.
3. The secret word or phrase must be *no longer than* ten letters.
4. Don't bother trying to cheat and send me gibberish. If I can't decrypt your message, before giving you your score of 5 I will require proof that the message really was a Vigenère cipher—that is, you must tell me what the secret word was and I will then check that I can in fact decrypt the message using the secret word.

Whether I succeed in decrypting your message or not, next week I can (if you like) explain how to go about trying to decrypt Vigenère ciphers without knowing the keyword.

There is more that could be said about modular arithmetic and cryptography. In particular, we haven't yet talked about public-key cryptography and the RSA system, which is the basis of much modern cryptography. For

example, your computer uses some variant of RSA every time you connect to a secure web site, like when you make a purchase from Amazon, so that no one observing the data being transmitted between your computer and Amazon can steal your credit card number.

If you find this cryptography stuff interesting, let me know and we could spend another week on it if you want.

