# MATH 157: Mathematics in the world
Notes 9 (February 26, 2019)

## Fermat's Little Theorem

If $p$ is a prime number and $a$ is an integer such that $(p, a) = 1$, then

$$a^{p-1} \equiv 1 \bmod p$$

.

### 1. When $p$ is not prime: example with 6

Is there a number $\phi(6)$ such that for every integer $a$ for which $(a, 6) = 1$, we have $a^{\phi(6)} \equiv 1 \bmod 6$?

### 2. When $p$ is not prime: example with 8

Is there a number $\phi(8)$ such that for every integer $a$ for which $(a, 8) = 1$, we have $a^{\phi(8)} \equiv 1 \bmod 8$?

### 3. Case $pq$

Given two different primes $p$ and $q$, is there a number $\phi(pq)$ such that for every integer $a$ for which $(a, pq) = 1$, we have $a^{\phi(pq)} \equiv 1 \bmod pq$?

### 4. One less than a perfect square

Find a prime number which is one less than a perfect square. How many can you find?

### 5. One more than a perfect square

Find a prime number which is one more than a perfect square. How many can you find?

## RSA encryption

In the second half of the class we will learn the RSA encryption method.

### 1. Follow up

Show that if we have two numbers $r, s$ such that $rs \equiv 1 \bmod (p-1)(q-1)$, we have

$$(a^r)^s \equiv a \bmod pq$$[1]

[1] Hint:what happens to $a^e$ when $e$ is a multiple of $(p-1)(q-1)$? And what if it has remainder 1 modulo $(p-1)(q-1)$?

## 2. Example

Given $r$, finding $s$ is a very complicated problem. Suppose $pq = 143$ and $r = 7$. Can you find an $s$ such that $rs \equiv 1 \bmod (p-1)(q-1)$?

## 3. The rules for RSA

So, here is how the RSA works.

| Public keys | Private key |
|---|---|
| $pq$ (but **not** $p$ and $q$)<br>the exponent $r$ | the exponent $s$ |

So, if you want to send a message containing the number $a$, you instead send a message containing

$$a^r \bmod pq,$$

that you can find easily using the public keys.
The only (efficient) way to recover $a$ from there is to raise $a^r$ to the $s$-th power, that can be done only by those in possess of the private key $s$.

## 4. Example

In the previous example, if we want to pass the message 5, we send the message

$$5^7 \bmod 143 = 132.$$

If you send around the number 132, nobody will be able to tell that you started from 5! Unless they know the answer to Problem 2.

## 5. More complicated example

Let us try a more complicated example! Let us consider $pq = 5561$, and $r = 17$. If you go on our Canvas website, under /Files/Programs, you will find a simple Python script that does the encryption for you. The file name is `encrypt.py`. Please download them now! Below the code for Python 3:

```
import sys

number = int(sys.argv[1])

encrypt = lambda x : pow(x,17,5561)

print("the encrypted number is %d" % (encrypt(number)))
```

Choose now a number $n$ smaller than 50 (to avoid too long computations). To find its encryption, please go to a Terminal window, place yourselves in your download directory, and type

```
python encrypt.py n
```

Of course, I possess a `decrypt.py` script that decrypts your numbers, I challenge you to find it too! (Only a regular calculator allowed...)

### 6. Bonus question

Why am I really asking for $n$ to be less than 50?

### 7. Challenge / Attendance question

I am going to annouce the date of the next attendance day in the following way. First I convert the message into a number using ASCII, and then apply the RSA encryption. The public keys:

$pq$ = 517455914919732254123656217032211531839094532369893229642571327645114307002144081368604993048475926293138350144785079510840260503724236454705586746991509190703407285942492559357950316199098929123854436863881449757322301807170117302776356126715070031755177228035358776919979307473542151731585234492632801366854921604291735105169432204108726816761137458091548471884379154580578353842608058217176523808771757672393415644857952738601523965233201875876367323531877985842000972464214144110086414534605032279572845555724439188718144774524529678519038768598913577 13

$r$ = 98698715324965192386409172309487128934678195123

Message = 38897417077019859509166236815914885759690424323247720289605162385160775068314259078280230982469271074174810178086887230626523936111137183336871318409012632114623533820886235750541962298387642294285355886509196352155820069888548536786150285460336584690605069970543397460433891418919409556100098838696329098237943499471573544513439941510907420784769964204725812601551973573228717527309237779781314390680100345773082249880240215516547318195489679030527094734330747698273436558294050488156561213009511350100686605267346638995061778065735773525246034488390999642

I challenge you to figure out the message! You may use whatever method you know, except for hacking into my computer. You may use `http://www.unit-conversion.info/texttools/ascii/` to convert text to numbers or numbers to text using ASCII. Feel free to send me encrypted email or encrypted Canvas post using the public keys given above to check if I truly possess the decrypt file!

When you encrypted your message, make the first character a lower case letter. This is to avoid start with 0 in the ASCII code, which will be discarded in the encryption file.

## Extra

### Number of 1 digits (given at a Google interview)

For $n$ positive integer, let $f(n)$ be the number of 1 digits that you need to write when writing all numbers from 1 to $n$ in base 10. For instance, $f(13) = 6$ because of **1**,1**0**,**11**,**12**,**13**. What is the first number bigger than 1 for which $f(n) = n$?

### Alternating number

We call a positive integer *alternating* if the digits are alternatively even and odd (for instance, 54769 is, 14320 is not). Find all positive integers $n$ that have a multiple that is alternating.