

## How Euclid, Fermat, and Euler Helped Modern Internet Security

Euclid (Born about 325 BC) is best known for his wonderful work in Geometry called “The Elements”. However, there is a little theorem in number theory of his that we are going to look at today. The theorem is about the search for the Greatest Common Divisor (GCD) between two numbers.

Method #1: Factor the two numbers. Let’s say we want to find the GCD between 28 and 98, let’s factor both:

$$28 = 4 \times 7 = 2 \times 2 \times 7 = 2^2 \times 7^1, \text{ while}$$

$$98 = 2 \times 49 = 2 \times 7 \times 7 = 2^1 \times 7^2. \text{ Now for each prime number, take the smallest exponent of the two:}$$

$$\text{GCD} = 2^1 \times 7^1 = 2 \times 7 = 14, \text{ so 14 is the largest divisor that is common to both 28 and 92.}$$

We’ll write this as  $(28, 98) = 14$

Here is another example. Find the GCD of 24, 36 and 60.

$$24 = 8 \times 3 = 2 \times 2 \times 2 \times 3 = 2^3 \times 3^1 \times 5^0, \text{ and}$$

$$36 = 4 \times 9 = 2 \times 2 \times 3 \times 3 = 2^2 \times 3^2 \times 5^0, \text{ and}$$

$$60 = 4 \times 15 = 2 \times 2 \times 3 \times 5 = 2^2 \times 3^1 \times 5^1. \text{ And if I take the smallest of each prime number, I get:}$$

$$\text{GCD} = 2^2 \times 3^1 \times 5^0 = 4 \times 3 \times 1 = 12. \text{ So } (24, 36, 60) = 12$$

Finally, let’s look at finding the GCD between 15 and 32

$$15 = 2^0 \times 3^1 \times 5^1, \text{ and}$$

$$32 = 2^5 \times 3^0 \times 5^0. \text{ And if I take the smallest of each prime number, I get:}$$

$\text{GCD} = 2^0 \times 3^0 \times 5^0 = 1 \times 1 \times 1$ , so  $(15, 32) = 1$ . The only number that divides into both 15 and 32 is 1. We say that 15 and 32 are “relatively prime”. Also,  $(n, 0) = n$  since “n” is a factor of both “n” and “0”.

Now, this is all very nice and easy if the numbers are small. What is needed in internet security is to find two numbers that are relatively prime, but the numbers may have 100 digits each! Numbers like this are very hard to factor, so the method described above is out. Before we see how Euclid solved this problem without factoring over 2 300 years ago, we must learn one new definition.

**Modulo:** The modulo of a number is the number left over (the remainder) after one number is divided by another. Let’s take 17 and divide it by 5. We get a quotient of 3 and a remainder of 2. Thus  $17 = 3 \times 5 + 2$ . We would write this the following way:  $17 \bmod 5 = 2$ . Another example,  $39 \bmod 7 = 4$ , since  $39 = 5 \times 7 + 4$ . Now  $\bmod 7$  is a great little arithmetic to find days of the week. Today is Friday, April 24, 2009. In 39 days the day of the week will be 4 days further along: Sat, Sun, Mon, Tuesday. So 39 days from now will be a Tuesday.

**Euclid’s Algorithm** (an algorithm is a method of working something out).

Let’s say that we are trying to find the GCD of two relatively small numbers, 4 950 and 420. Obviously 10 goes into both, but is there a larger common divisor? And can we do this without factoring?

Euclid found that  $(m, n) = (n, m \bmod n)$ , so  $(4\,950, 420) = (420, 4\,950 \bmod 420)$ . Well  $4\,950 \bmod 420 = 330$ , since  $4\,950 = 420 \times 11 + 330$ . So, we now have simplified the problem to  $(420, 330)$ . Let’s continue this:

$$(420, 330) = (330, 420 \bmod 330) \text{ and since } 420 = 330 \times 1 + 90, \text{ this becomes } (330, 90),$$

$$(330, 90) = (90, 330 \bmod 90) \text{ and since } 330 = 90 \times 3 + 60, \text{ this becomes } (90, 60). \text{ At this time you might see that}$$

$(90, 60) = 30$ , and you have your answer. However, let’s assume you do not notice this, (or that you are a computer):

$$(90, 60) = (60, 90 \bmod 60) \text{ and since } 90 = 60 \times 1 + 30, \text{ this becomes } (60, 30).$$

$(60, 30) = (30, 60 \bmod 30)$  and since  $60 = 2 \times 30 + 0$ , this becomes  $(30, 0)$  which, as we saw above, was equal to 30.

Putting it all together we get:

$$(4\ 950, 420) = (420, 330) = (330, 90) = (90, 60) = (60, 30) = (30, 0) = 30.$$

So  $(4\ 950, 420) = 30$ . This is all done with NO factoring, and with a simple algorithm that can be easily programmed on a computer, or a spreadsheet. You continue going until the second number in the bracket becomes a 0, and then your answer is the first number in the same bracket.

What cryptographic systems want for internet, and other, security, is to find two very large numbers of at least 100 digits or more, where  $(m, n) = 1$ . In other words they are “relatively prime”. Euclid’s Algorithm is a very useful method for them. This shows how something worked out in math, may be of little use at that time, but of major use in later years.

The work above and below I got from Sarah Flannery’s wonderful book, called *In Code*, by Workman Publishing, New York.

### **Fermat, Euler and RSA**

Both Fermat (French mathematician 1601 – 1665) and Euler (Swiss mathematician, 1707 – 1783) had a tremendous body of work each, but two little theorems are key to modern cryptographic systems.

First of all a new symbol:  $\phi(n)$  stands for the number of numbers less than “n” that are relatively prime to “n”. So  $\phi(12) = 4$ , since 1, 5, 7 and 11 are relatively prime to 12. Also  $\phi(p) = p - 1$ , if “p” is a prime number.

In 1640 Fermat found that, if “p” is any prime number,  $a^{p-1} = 1 \pmod{p}$ , while in 1736 Euler extended this to:

If “n” is any natural number, then:  $a^{\phi(n)} = 1 \pmod{n}$  for every natural number “a” satisfying  $(a, n) = 1$ .

Thus Euler’s theorem generalizes Fermat’s theorem. Now how does this fit in to modern cryptographic systems? The first public key cryptosystem was invented by Ronald Rivest, Adi Shamir, and Leonard Adleman at MIT in 1977. It became known as the RSA (the first letters of their last names) system and today is recognized as a standard of encryption worldwide.

Flannery’s book (and I am sure, the internet) details this scheme on pages 272 to 273. It involves 2 random prime numbers “p” and “q” (very large), their product “n”,  $\phi(n)$ , another random number  $e < \phi(n)$ , so that we have  $(e, \phi(n)) = 1$  and modulo arithmetic. So Euclid, Fermat, Euler have all been part of working out the modern RSA encryption algorithm. It was first published in the Scientific American August 1977 issue.

So, to paraphrase Newton, we really do stand on the shoulders of those who have gone before us, in order to “see” further.