THE MAGIC OF NUMBERS

FLORIAN ENESCU

1. Introduction

The world of numbers has captured the imagination of many people since ancient times. This talk will present some of the elementary properties of numbers together with some of their classical and fascinating aspects. We hope to give a glimpse of this beautiful world by studying basic and, apparently, simple questions about integers. We will see that some of the questions can be answered with elementary techniques, some will prove to be more difficult, while for some an answer is not yet known. However, all these questions share an intrinsic beauty. More significantly, they also lead to important applications to our everyday life, such as cryptography.

We will start with a few simple questions that can be answered with a little work:

Definition 1.1. A positive integer is called a *perfect square* if it can be written as the square of an integer.

Question 1.2. *Which of the following numbers are perfect squares?*
$15, 34, 64, 324, 7897, 16757894327, 625$

Definition 1.3. A positive integer $p > 1$ is prime if the only positive divisors of p are 1 and p. If p is not prime, then it is said to be composite.

Question 1.4. *Which of the following numbers are prime?*
$67, 34, 59, 881, 134571$

Question 1.5. *Assume you have two coins. Coin A values* 3 *cents and coin B values* 5 *cents. Is it true that you can pay out any large enough amount of money by using only coins of types A and B? How about if the coins have values equal to* 5 *and respectively* 7*?*

2. Prime numbers, divisibility

One of the very first things that we learn when we play with numbers is how to divide one number by another. This fact is summarized in the following result, which is assumed familiar to the reader.

Theorem 2.1. *Given two integers a and b with $b \neq 0$, there exists unique integers q and r such that*

$$a = bq + r$$

and $0 \leq r < |b|$. (The number q is called the quotient of the division of a by b, while r is the remainder.)

Let us discuss the representation of any number n in base 10. Divide n by 10: $n = q10 + r_0$ with q_0 unique such that it is positive and less than 10. Divide q by 10: $q = 10q_1 + r_1$, where again r_1 is unique with $0 \leq r_1 < 10$. So, $n = 10^2 q_1 + 10r_1 + r_0$. Continue the procedure until you can write

$$n = 10^k r_k + 10^{k-1} r_{k-1} + \cdots + 10r_1 + r_0$$

with $0 \leq r_i < 10$. This representation is unique because at each step the remainder is unique. It should be kept in mind that the way we write numbers on paper is really only their representation in base 10. They might have different representations in other bases. For example, write 101 in base 2.

Problem 2.2. *Prove that any number is divisible by 9 if the sum of its digits (of its representation in base 10) is divisible by 9.*

Proof. Write n in base 10:

$$n = 10^k r_k + 10^{k-1} r_{k-1} + \cdots + 10r_1 + r_0.$$

But $10 = 9 + 1$, and so, for every h positive integer, 10^h is of the form $9h' + 1$, where h' is some integer. Therefore, $n = 9s + r_k + \cdots + r_0$ and hence $9|n$ if and only if $9|r_k + \cdots r_0$ which is the statement of the problem.

□

We can see that in the proof given above that it is important that 10^h equals 1 plus a certain multiple of 9, but the value of the multiple is not important. This is the same as thinking that 10 equals 1 as far as we are concerned with the divisibility by 9. Let us express this in a correct mathematical way.

Definition 2.3. Let n a positive integer. We say that a is *congruent* to b *modulo* n if and only if $n|a - b$. We will write this $a \equiv b \pmod{n}$.

So, modulo 9 there are really only nine numbers : $0, 1, 2, 3, 4, 5, 6, 7, 8$. Also, modulo 2 there are only two numbers: 0, 1 which is the same as saying that a number is either even or odd. Our clocks use numbers modulo 12.

One can check that a perfect square is congruent to $0, 1, 4, 5, 6, 9$ modulo 10. Hence, Question 1.2 can be answered easily now as the numbers that have the last digit equal to 7 cannot be perfect squares.

Let us move on to a simple and natural question. How do we check that a number is prime? If the number is large then the definition of prime numbers seems to saying that we need to check that all the numbers from 2 up to $p-1$ do not divide p.

Proposition 2.4. *A number $p > 0$ is prime if and only if it is not divisible by any prime q, $1 < q \leq \sqrt{p}$.*

Proof. If p is not prime then there is a prime p' that divides p: $p = p' \cdot a$. But then either $p' \leq \sqrt{p}$ or $a \leq \sqrt{p}$. Assume that $a \leq \sqrt{p}$, since otherwise we are done, and repeat the procedure. It follows that, eventually, there is a prime $q \leq \sqrt{p}$ such that $q|p$. □

This criterion is indeed useful: one can show that 881 by checking that the prime numbers up to 30 do not divide 881 (the prime numbers less than 30 are $2,\ 3, 5, 7, 11, 13, 17, 19, 23, 29$.) This way we can also answer Question 1.4.

Definition 2.5. Let a and b two positive integers. The largest number d that divides both of them is called their greatest common divisor. It is denoted by $\gcd(a, b)$.

Problem 2.6. *Find the greatest common divisor for the following pairs:* 8 *and* 62, 56 *and* 124.

Proposition 2.7. *To compute the greatest common divisor of two numbers a and b, let $r_{-1} = a$ and let $r_0 = b$, and compute the successive quotients and remainders*

$$r_{i-1} = q_{i+1} r_i + r_{i+1}$$

for $i = 0, 1, 2, 3, ...$ until we get some remainder r_{n+1} equal to 0. The last nonzero remainder r_n is then the greatest common divisor of a and b.

Proof. Let d a common divisor for a and b. At every step, d divides r_{i-1} and r_i and so d divides r_{i+1}. In conclusion, d divides r_n and, so, it remains to be shown that r_n divides a and b and that the Euclidean Algorithm finishes.

To prove that r_n divides a and b start from the bottom up. First, r_n divides r_{n-1} (since $r_{n+1} = 0$). So, r_n divides $r_{n-2} = q_n r_{n-1} + r_n$ and can continue until it we see that r_n divides all r_i, including a and b.

The algorithm ends because $r_{i+1} < r_i$ for all i so at some point the remainder must become zero. □

Problem 2.8. *Compute* $\gcd(22, 60)$ *and* $\gcd(1160718174, 316258250)$.

Proof. We will compute $\gcd(1160718174, 316258250)$:

$$1160718174 = 3 \cdot 316258250 + 211943424$$

$$316258250 = 1 \cdot 211943424 + 104314826$$

$$211943424 = 2 \cdot 104314826 + 3313772$$

$$104314826 = 3 \cdot 3313772 + 1587894$$

$$3313772 = 2 \cdot 1587894 + 137984$$

$$1587894 = 11 \cdot 137984 + 70070$$

$$137984 = 1 \cdot 70070 + 67914$$

$$70070 = 1 \cdot 67914 + 2156$$

$$67914 = 31 \cdot 2156 + 1078$$

$$2156 = 2 \cdot 1078 + 0$$

So, the greatest common divisor is 1078.

□

Question 2.9. *What is the smallest positive value of* $5x + 3y$*, where* x *and* y *are arbitrary integers? How about* $7x + 3y$*? How about* $6x + 2y$*?*

Experiment with numbers and conjecture the following Theorem:

Theorem 2.10. *Let* a *and* b *two positive integers. The smallest positive value of* $ax + by$ *is equal to* $\gcd(a, b)$*, where* x *and* y *are some integers.*

Proof. One can deduce this from the Euclidean Algorithm. How? □

Proposition 2.11. *Let* p *be a prime number. Show that if* $p|ab$*, with* a *and* b *integers, then* $p|a$ *or* $p|b$*.*

Proof. Assume that p does not divide a. So $\gcd(a, p) = 1$. Hence there exist integers x and y such that $ax + py = 1$. Multiply by b in both sides note that since $p|abx$ and $p|py$, then $p|b$.

□

Proposition 2.12. *Every positive integer greater than* 1 *can be decomposed as a product of prime numbers. The decomposition is unique up to permuting the terms.*

Proof. Let n be a positive integer. It it is prime we are done. If not write $n = ab$ where $a < n$ and $b < n$ for obvious reasons. If a and b are both prime, we are again done. If not, continue by factorizing a and b. Since the factors are always less than the number we are factorizing, the procedure will stop eventually, and, then, n will be written as a product of primes.

Uniqueness: write $n = p_1 \cdots p_k = q_1 \cdots q_h$ two prime factorizations of n. Since p_1 divides n, then it must divide one of the $q's$. Say $p_1|q_1$; since q_1 is prime, then $p_1 = q_1$. Cancel it in both factorizations and continue until $k = h$ and $p_i = q_i$ for all $i = 1, \cdots, k$. □

Use the above Theorem to solve Question 3 from the Introduction.

Theorem 2.13. *Prove that there are infinitely many prime numbers. Prove that there are infinitely many prime numbers of the form* $4m+3$ *with* m *positive integer.*

Proof. The first part is well known, so we will do only the second part. the idea is similar to the behind the proof of the first part.

Assume that there are only finitely many primes of the form $4m+3$ with m positive integer. List all of them

$$3, p_1, ..., p_k$$

and look at $4p_1 \cdots p_k + 3$. It cannot be prime, since it is bigger than those listed already. Write its prime factorization. It is easy to see that at least one of the primes of this factorization must be congruent to 3 modulo 4. But this means that $p = 3$ or $p = p_i$ for some i. If $p = 3$ then since $p|4p_1 \cdots p_k + 3$, we get that $p|p_1 \cdots p_k$ which is impossible. We get a similar contradiction if $p = p_i$.

In conclusion there must be finitely many primes of the form $4m+3$ with m positive integer. □

State Dirichlet's Theorem.

Theorem 2.14 (Dirichlet, 1837)**.** *Let* a *and* m *be integers with* $\gcd(a, b) = 1$. *Then there are infinitely many primes that are congruent to* a *modulo* m.

Problem 2.15. *Is* $2^{58} + 1$ *a composite number or not? Can you write a factorization of it?*

Proof. Note that $2^{4n+2}+1 = (2^{2n+1}-2^{n+1}+1)(2^{2n+1}+2^{n+1}+1)$. It can be seen that 5 divides our number in a different way. However this method will not provide a factorization of $2^{58}+1$. Indeed, $2^{58}+1 = 4^{29}+1$ and now we can see that $1-(-4) = 5$ divides $1+4^{29} = 1-(-4)^{29}$. □

Problem 2.16. *Prove that 2^h+1 prime implies that h is a power of 2.*

Primes of the form $2^{2^k}+1$ are called *Fermat primes*. Denote $F_k = 2^{2^k}+1$. Fermat believed that these numbers are all primes. However, Euler showed that $F_5 = 641 \cdot 6700417$.

Problem 2.17. *Show that* $\gcd(F_n, F_m) = 1$ *if* $n \neq m$.

Proof. Hint: Show that $F_m | F_n - 2$ if $n > m$. □

Problem 2.18. *Show that if a^n-1 is prime then $a = 2$ and n is prime. Are all the numbers of the form 2^p-1, p prime, prime numbers? Prove or disprove. (Hint: let $p = 11$.)*

Primes of the form 2^p-1 are called Mersenne primes. It is not known if there are infinitely many numbers of this form. In 1999, Hajratwala proved that for $p = 6972593$ (which is prime), 2^p-1 is prime.

We will close this section by listing a few questions.

Is it true that there are infinitely many prime numbers p such that $p+2$ is also prime? This is believed to be true and the statement is called *The Twin primes conjecture*. The best result up to date is that of Chen Jing-run that showed that there are infinitely many primes p so that $p+2$ is either prime or a product of primes.

Is it true that every even number greater or equal to 4 is the sum of two primes? This is believed to be true and it is called Goldbach conjecture. I. M. Vinogradov proved (1937) that any sufficiently large odd number is a sum of three primes. Chen Jing-run showed in 1966 that every even number n is a sum of two numbers p prime, and a prime or a product of two primes.

Are there infinitely many primes of the form n^2+1, with n integer? Iwaniec proved in 1978 that there are infinitely many values n such that n^2+1 is prime or a product of two primes.

Fix $n \geq 2$. What are the numbers a, b, c such that $a^n+b^n = c^n$? Wiles has confirmed a conjecture of Fermat that says that for $n \geq 3$ there are no such numbers a, b, c. Wiles work is deep and relies of contributions of about two dozens of other mathematicians. This result is called the Fermat's Last Theorem. For $n = 2$, it turns out that one describes all the triples (a, b, c) in an elementary fashion.

3. Pythagorean numbers

We all know from geometry that in a right triangle with hypotenuse c and sides a and b the relation $a^2+b^2=c^2$ holds. Such a triple (a,b,c) is called a Pythagorean triple. We would like to find all such triples of integers (a,b,c).

First note that if there is a positive integer d that divides a, b, and c, then we can cancel it out for both sides of the equations. This means that we should study the equation

$$a^2+b^2=c^2,$$

where a, b, c do not share a common divisor. These triples are called primitive Pythagorean triples.

First, what can we say about the parity of a, b, c?

Let us look at some Pythagorean triples: $(3,4,5)$, $(5,12,13)$, $(8,15,17)$, $(28,45,53)$. It seems a and b have different parity, while c is always odd. Let us try to prove this.

First, if a and b are both even, then c is even too. False, since 2 would then divide all three numbers.

Assume that a and b are both odd: $a=2x+1, b=2y+1$. It follows that c is even, hence $c=2z$. Plug this into the equation and reduce the expression to

$$2x^2+2x+2y^2+2y+1=2z.$$

Clearly this is impossible and so, we have proven our assertion.

We concentrate on the equation

$$a^2+b^2=c^2$$

with a odd, b even, a,b,c having no common factor.

Clearly, $a^2=(c-b)(c+b)$. Check a few examples. What do you notice?

Let us prove that, indeed, $c+b$ and $c-b$ are indeed squares. First, note that in all examples $c+b$ and $c-b$ do not have common divisors. Proving this is easier: if d divides both numbers, then d divides $2c$ and $2b$. Since d is different than 2, then d divides b and c. But then d divides a, too which is false.

So, $c+b$ and $c-b$ do not have a common divisor and their product is a square. This means that $c+b$ and $c-b$ are both squares! This can be seen from their factorization into primes.

So, $c-b=s^2$ and $c+b=t^2$, with $s>t\geq 0$ are odd integers with no common factors. This shows that $a=st$, $b=\frac{s^2-t^2}{2}$ and $c=\frac{s^2+t^2}{2}$, where s and t are integers. It is easy to check that for each s, and t one gets a Pythagorean triple.

For example, let s be an arbitrary odd number and $t = 1$. Then $c = b + 1$ and this explains why this holds true in some examples.

There is another way of determining the Pythagorean triples: by geometry!

Divide the Pythagorean equation by c^2. So, $(a/c)^2 + (b/c)^2 = 1$. So let us solve first the equation

$$x^2 + y^2 = 1$$

in rational numbers.

Take the point $(-1, 0)$ which lies on the unit circle. Consider a line through it of rational slope m: $y = m(x + 1)$. We will show that the other point of intersection between this line and our circle has rational coordinates. It is of course a solution of our equation. On the other hand, if (x, y) is on the circle and it has rational coordinates, then the line joining the point with $(-1, 0)$ has a rational slope. In conclusion, all rational points on the circle (i.e., our solutions), except $(-1, 0)$, are obtained by intersecting the unit circle with a line of rational slope through $(-1, 0)$.

Let us compute the intersection between $x^2 + y^2 = 1$ and $y = m(x + 1)$. A few manipulations will give:

$x = \frac{m^2-1}{m^2+1}$ and $y = \frac{2m}{m^2+1}$.

In fact, if we write $m = u/v$ with $(u, v) = 1$, we get that

$$(x, y) = (\frac{u^2 - v^2}{u^2 + v^2}, \frac{2uv}{u^2 + v^2}).$$

Now, by clearing the denominators will see that any Pythagorean triple is of the form $(u^2 - v^2, 2uv, u^2 + v^2)$.

What is the relation between this description and the one we gave in our first solution to the problem?

Remark 3.1. The books listed in the bibliography have been used in the preparation of these notes. They contain information on many other aspects of elementary number theory which are recommended to the interested reader.

References

[1] R. Kumanduri, C. Ramero, *Number Theory with Computer Applications*, Prentice Hall, 1998.

[2] I. Peterson, *The Mathematical Tourist*, Chapter 2, W. H. Freeman and Company, 1998.

[3] J. H. Silverman, *A Friendly Introduction to Number Theory*, Prentice Hall, 2001.