Introduction to number theory-4

April 3, 2017

Bertrand's Postulate

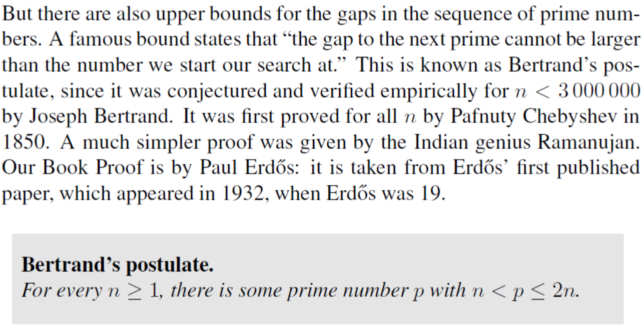
We have seen that the sequence of prime numbers $2, 3, 5, 7, \dots$ is infinite. To see that the size of its gaps is not bounded, let $N := 2 \cdot 3 \cdot 5 \cdots p$ denote the product of all prime numbers that are smaller than $k + 2$, and note that none of the k numbers

$$N + 2, N + 3, N + 4, \dots, N + k, N + (k + 1)$$

is prime, since for $2 \leq i \leq k + 1$ we know that i has a prime factor that is smaller than $k + 2$, and this factor also divides N, and hence also $N + i$. With this recipe, we find, for example, for $k = 10$ that none of the ten numbers

$$2312, 2313, 2314, \dots, 2321$$

is prime.



But there are also upper bounds for the gaps in the sequence of prime numbers. A famous bound states that "the gap to the next prime cannot be larger than the number we start our search at." This is known as Bertrand's postulate, since it was conjectured and verified empirically for $n < 3\,000\,000$ by Joseph Bertrand. It was first proved for all n by Pafnuty Chebyshev in 1850. A much simpler proof was given by the Indian genius Ramanujan. Our Book Proof is by Paul Erdős: it is taken from Erdős' first published paper, which appeared in 1932, when Erdős was 19.

Bertrand's postulate.
For every $n \geq 1$, there is some prime number p with $n < p \leq 2n$.

Proof. We will estimate the size of the binomial coefficient $\binom{2n}{n}$ carefully enough to see that if it didn't have any prime factors in the range $n < p \leq 2n$, then it would be "too small." Our argument is in five steps.

(1) We first prove Bertrand's postulate for $n < 4000$. For this one does not need to check 4000 cases: it suffices (this is "Landau's trick") to check that

$$2, 3, 5, 7, 13, 23, 43, 83, 163, 317, 631, 1259, 2503, 4001$$

is a sequence of prime numbers, where each is smaller than twice the previous one. Hence every interval $\{y : n < y \leq 2n\}$, with $n \leq 4000$, contains one of these 14 primes.

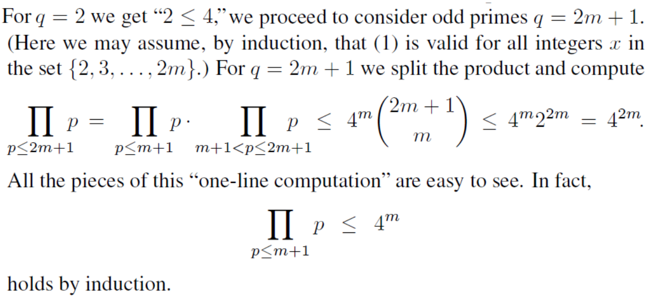
(2) Next we prove that

$$\prod_{p \le x} p \;\le\; 4^{x-1} \qquad \text{for all real } x \ge 2, \tag{1}$$

where our notation — here and in the following — is meant to imply that the product is taken over all *prime* numbers $p \le x$. The proof that we present for this fact uses induction on the number of these primes. It is not from Erdős' original paper, but it is also due to Erdős (see the margin), and it is a true Book Proof. First we note that if q is the largest prime with $q \le x$, then

$$\prod_{p \le x} p = \prod_{p \le q} p \qquad \text{and} \qquad 4^{q-1} \le 4^{x-1}.$$

Thus it suffices to check (1) for the case where $x = q$ is a prime number.



For $q = 2$ we get “$2 \leq 4$,”we proceed to consider odd primes $q = 2m + 1$. (Here we may assume, by induction, that (1) is valid for all integers x in the set $\{2, 3, \ldots, 2m\}$.) For $q = 2m + 1$ we split the product and compute

$$\prod_{p \leq 2m+1} p = \prod_{p \leq m+1} p \cdot \prod_{m+1 < p \leq 2m+1} p \;\leq\; 4^m \binom{2m+1}{m} \;\leq\; 4^m 2^{2m} \;=\; 4^{2m}.$$

All the pieces of this “one-line computation” are easy to see. In fact,

$$\prod_{p \leq m+1} p \;\leq\; 4^m$$

holds by induction.

The inequality

$$\prod_{m+1<p\leq 2m+1} p \;\leq\; \binom{2m+1}{m}$$

follows from the observation that $\binom{2m+1}{m} = \frac{(2m+1)!}{m!(m+1)!}$ is an integer, where the primes that we consider all are factors of the numerator $(2m+1)!$, but not of the denominator $m!(m+1)!$. Finally

$$\binom{2m+1}{m} \;\leq\; 2^{2m}$$

holds since

$$\binom{2m+1}{m} \text{ and } \binom{2m+1}{m+1}$$

are two (equal!) summands that appear in

Legendre's theorem

The number $n!$ contains the prime factor p exactly

$$\sum_{k\geq 1}\left\lfloor \frac{n}{p^k}\right\rfloor$$

times.

■ **Proof.** Exactly $\lfloor \frac{n}{p} \rfloor$ of the factors of $n! = 1 \cdot 2 \cdot 3 \cdots n$ are divisible by p, which accounts for $\lfloor \frac{n}{p} \rfloor$ p-factors. Next, $\lfloor \frac{n}{p^2} \rfloor$ of the factors of $n!$ are even divisible by p^2, which accounts for the next $\lfloor \frac{n}{p^2} \rfloor$ prime factors p of $n!$, etc. □

(3) From Legendre's theorem (see the box) we get that $\binom{2n}{n} = \frac{(2n)!}{n!n!}$ contains the prime factor p exactly

$$\sum_{k\geq 1}\left(\left\lfloor \frac{2n}{p^k}\right\rfloor - 2\left\lfloor \frac{n}{p^k}\right\rfloor\right)$$

times. Here each summand is at most 1, since it satisfies

$$\left\lfloor \frac{2n}{p^k}\right\rfloor - 2\left\lfloor \frac{n}{p^k}\right\rfloor \;<\; \frac{2n}{p^k} - 2\left(\frac{n}{p^k} - 1\right) \;=\; 2,$$

and it is an integer. Furthermore the summands vanish whenever $p^k > 2n$. Thus $\binom{2n}{n}$ contains p exactly

$$\sum_{k\geq 1}\left(\left\lfloor \frac{2n}{p^k}\right\rfloor - 2\left\lfloor \frac{n}{p^k}\right\rfloor\right) \;\leq\; \max\{r : p^r \leq 2n\}$$

times. Hence the largest power of p that divides $\binom{2n}{n}$ is not larger than $2n$. In particular, primes $p > \sqrt{2n}$ appear at most once in $\binom{2n}{n}$.

Furthermore — and this, according to Erdős, is the key fact for his proof — primes p that satisfy $\frac{2}{3}n < p \leq n$ do not divide $\binom{2n}{n}$ at all! Indeed, $3p > 2n$ implies (for $n \geq 3$, and hence $p \geq 3$) that p and $2p$ are the only multiples of p that appear as factors in the numerator of $\frac{(2n)!}{n!n!}$, while we get two p-factors in the denominator.

Examples such as

$$\binom{26}{13} = 2^3 \cdot 5^2 \cdot 7 \cdot 17 \cdot 19 \cdot 23$$

$$\binom{28}{14} = 2^3 \cdot 3^3 \cdot 5^2 \cdot 17 \cdot 19 \cdot 23$$

$$\binom{30}{15} = 2^4 \cdot 3^2 \cdot 5 \cdot 17 \cdot 19 \cdot 23 \cdot 29$$

illustrate that "very small" prime factors $p < \sqrt{2n}$ can appear as higher powers in $\binom{2n}{n}$, "small" primes with $\sqrt{2n} < p \leq \frac{2}{3}n$ appear at most once, while factors in the gap with $\frac{2}{3}n < p \leq n$ don't appear at all.

(4) Now we are ready to estimate $\binom{2n}{n}$. For $n \geq 3$, using an estimate from page 12 for the lower bound, we get

$$\frac{4^n}{2n} \leq \binom{2n}{n} \leq \prod_{p \leq \sqrt{2n}} 2n \quad \cdot \prod_{\sqrt{2n} < p \leq \frac{2}{3}n} p \quad \cdot \prod_{n < p \leq 2n} p$$

and thus, since there are not more than $\sqrt{2n}$ primes $p \leq \sqrt{2n}$,

$$4^n \leq (2n)^{1+\sqrt{2n}} \cdot \prod_{\sqrt{2n} < p \leq \frac{2}{3}n} p \quad \cdot \prod_{n < p \leq 2n} p \qquad \text{for} \quad n \geq 3. \qquad (2)$$

(5) Assume now that there is no prime p with $n < p \leq 2n$, so the second product in (2) is 1. Substituting (1) into (2) we get

$$4^n \;\leq\; (2n)^{1+\sqrt{2n}}\, 4^{\frac{2}{3}n}$$

or

$$4^{\frac{1}{3}n} \;\leq\; (2n)^{1+\sqrt{2n}}, \qquad (3)$$

which is false for n large enough! In fact, using $a + 1 < 2^a$ (which holds for all $a \geq 2$, by induction) we get

$$2n = \big(\sqrt[6]{2n}\big)^6 < \big(\lfloor \sqrt[6]{2n} \rfloor + 1\big)^6 < 2^{6\lfloor \sqrt[6]{2n} \rfloor} \leq 2^{6\sqrt[6]{2n}}, \qquad (4)$$

and thus for $n \geq 50$ (and hence $18 < 2\sqrt{2n}$) we obtain from (3) and (4)

$$2^{2n} \leq (2n)^{3\left(1+\sqrt{2n}\right)} < 2^{\sqrt[6]{2n}\left(18+18\sqrt{2n}\right)} < 2^{20\sqrt[6]{2n}\sqrt{2n}} = 2^{20(2n)^{2/3}}.$$

This implies $(2n)^{1/3} < 20$, and thus $n < 4000$. □

A Linear Diophantine Equation

1.6 A Linear Diophantine Equation

A *diophantine equation* is an equation of the form

$$f(x_1, \ldots, x_k) = b$$

that we want to solve in rational numbers, integers, or nonnegative integers. This means that the values of the variables $x_1, \ldots, x_k$ will be rationals, integers, or nonnegative integers. Usually the function $f(x_1, \ldots, x_k)$ is a polynomial with rational or integer coefficients.

In this section we consider the linear diophantine equation

$$a_1x_1 + \cdots + a_kx_k = b.$$

We want to know when this equation has a solution in integers, and when it has a solution in nonnegative integers. For example, the equation

$$3x_1 + 5x_2 = b$$

has a solution in integers for every integer b, and a solution in nonnegative integers for $b = 0, 3, 5, 6$, and all $b \geq 8$ (Exercise 20).

Theorem 1.15 *Let $a_1, \ldots, a_k$ be integers, not all zero. For any integer b, there exist integers $x_1, \ldots, x_k$ such that*

$$a_1x_1 + \cdots + a_kx_k = b \tag{1.4}$$

if and only if b is a multiple of $(a_1, \ldots, a_k)$. In particular, the linear equation (1.4) has a solution for every integer b if and only if the numbers $a_1, \ldots, a_k$ are relatively prime.

Proof. Let $d = (a_1, \ldots, a_k)$. If equation (1.4) is solvable in integers x_i, then d divides b since d divides each integer a_i. Conversely, if d divides b, then $b = dq$ for some integer q. By Theorem 1.4, there exist integers $y_1, \ldots, y_k$ such that

$$a_1y_1 + \cdots + a_ky_k = d.$$

Let $x_i = y_iq$ for $i = 1, \ldots, k$. Then

$$a_1x_1 + \cdots + a_kx_k = a_1(y_1q) + \cdots + a_k(y_kq) = dq = b$$

is a solution of (1.4). It follows that (1.4) is solvable in integers for every b if and only if $(a_1, \ldots, a_k) = 1$. □

Theorem 1.16 *Let $a_1, \ldots, a_k$ be positive integers such that*

$$(a_1, \ldots, a_k) = 1.$$

If

$$b \geq (a_k - 1) \sum_{i=1}^{k-1} a_i,$$

then there exist nonnegative integers $x_1, \ldots, x_k$ such that

$$a_1 x_1 + \cdots + a_k x_k = b.$$

Proof. By Theorem 1.15, there exist integers $z_1, \ldots, z_k$ such that

$$a_1 z_1 + \cdots + a_k z_k = b.$$

Using the division algorithm, we can divide each of the integers $z_1, \ldots, z_{k-1}$ by a_k so that

$$z_i = a_k q_i + x_i$$

and

$$0 \leq x_i \leq a_k - 1$$

for $i = 1, \ldots, k-1$. Let $\quad x_k = z_k + \sum_{i=1}^{k-1} a_i q_i.$

Then

$$\begin{aligned}
b &= a_1z_1 + \cdots + a_{k-1}z_{k-1} + a_kz_k \\
&= a_1(a_kq_1 + x_1) + \cdots + a_{k-1}(a_kq_{k-1} + x_{k-1}) + a_kz_k \\
&= a_1x_1 + \cdots + a_{k-1}x_{k-1} + a_k\left(z_k + \sum_{i=1}^{k-1} a_iq_i\right) \\
&= a_1x_1 + \cdots + a_{k-1}x_{k-1} + a_kx_k \\
&\leq (a_k - 1)\sum_{i=1}^{k-1} a_i + a_kx_k,
\end{aligned}$$

where x_k is an integer, possibly negative. However, if

$$b \geq (a_k - 1)\sum_{i=1}^{k-1} a_i,$$

then $a_kx_k \geq 0$ and so $x_k \geq 0$. This completes the proof. □

Let $a_1, \ldots, a_k$ be relatively prime positive integers. Since every sufficiently large integer can be written as a nonnegative integral linear combination of $a_1, \ldots, a_k$, it follows that there exists a smallest integer

$$G(a_1, \ldots, a_k)$$

such that every integer $b \geq G(a_1, \ldots, a_k)$ can be represented in the form (1.4), where the variables $x_1, \ldots, x_k$ are nonnegative integers. The example above shows that

$$G(3, 5) = 8.$$

The *linear diophantine problem of Frobenius* is to determine $G(a_1, \ldots, a_k)$ for all finite sets of relatively prime positive integers $a_1, \ldots, a_k$. This is a difficult open problem, but there are some special cases where the solution is known. The following theorem solves the Frobenius problem in the case $k = 2$.

Theorem 1.17 *Let a_1 and a_2 be relatively prime positive integers. Then*

$$G(a_1, a_2) = (a_1 - 1)(a_2 - 1).$$

Proof. We saw in the proof of Theorem 1.15 that for every integer b there exist integers x_1 and x_2 such that

$$b = a_1x_1 + a_2x_2 \qquad \text{and} \qquad 0 \leq x_1 \leq a_2 - 1. \tag{1.5}$$

If we have another representation

$$b = a_1x_1' + a_2x_2', \qquad \text{and} \qquad 0 \leq x_1' \leq a_2 - 1,$$

then

$$a_1(x_1 - x_1') = a_2(x_2' - x_2).$$

Since a_2 divides $a_1(x_1 - x_1')$ and $(a_1, a_2) = 1$, Euclid's lemma implies that a_2 divides $x_1 - x_1'$. Then $x_1 = x_1'$, since $|x_1 - x_1'| \leq a_2 - 1$. It follows that $x_2 = x_2'$, and so the representation (1.5) is unique.

If the integer b *cannot* be represented as a nonnegative integral combination of a_1 and a_2, then we must have $x_1 \leq -1$ in the representation (1.5). This implies that

$$b = a_1x_1 + a_2x_2 \leq a_1(a_2 - 1) + a_2(-1) = (a_1 - 1)(a_2 - 1) - 1,$$

and so $G(a_1, a_2) \leq (a_1 - 1)(a_2 - 1)$. On the other hand, since

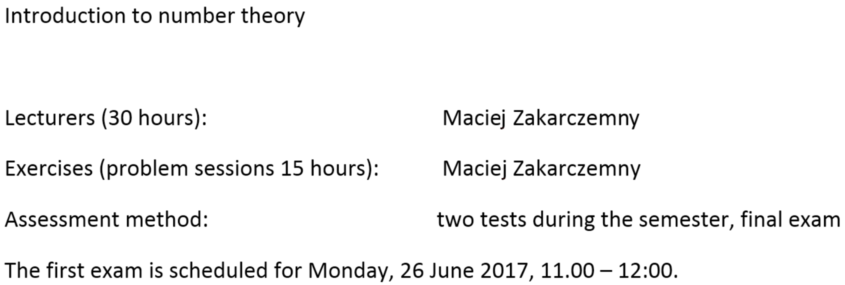
$$a_1(a_2 - 1) + a_2(-1) = a_1a_2 - a_1 - a_2 < a_1a_2,$$

it follows that if

$$a_1a_2 - a_1 - a_2 = a_1x_1 + a_2x_2$$

for any nonnegative integers x_1 and x_2, then $0 \leq x_1 \leq a_2 - 1$. By the uniqueness of the representation (1.5), we must have $x_1 = a_2 - 1$ and $x_2 = -1$. Therefore, the integer $a_1a_2 - a_1 - a_2$ cannot be represented as a nonnegative integral linear combination of a_1 and a_2, and so $G(a_1, a_2) = (a_1 - 1)(a_2 - 1)$. □

thank you



Introduction to number theory

Lecturers (30 hours):	Maciej Zakarczemny
Exercises (problem sessions 15 hours):	Maciej Zakarczemny
Assessment method:	two tests during the semester, final exam

The first exam is scheduled for Monday, 26 June 2017, 11.00 – 12:00.

Lectures and a lists of exercises (exercises sheets) will be available online.

My website:	maciej.zakarczemny.pl
tab:	Introduction to number theory

Topics covered:

Notation and Conventions

Divisibility, GCD, factorization

Fundamental Theorem of Arithmetic

Congruences

Fermat’s Little Theorem

Euler’s Phi function.

Prime numbers; counting primes, Mersenne and other types of primes

Carmichael numbers

Modular arithmetic and algebra, Chinese Remainder Theorem.

Diophantine equations.

Pythagorean Triples and the Fermat’s Last Theorem

“Unbreakable” codes and other applications.

Books:

J. Silverman, A friendly introduction to Number Theory, Prentice Hall, 1997.

Shoup, V. A Computational Introduction to Number Theory and Algebra.

Available at: http://shoup.net/ntb/ntb-v2.pdf

K. Ireland, M. Rosen, A classical introduction in modern number theory, Springer 1990.

W.Narkiewicz, Number Theory, World Scientific, Singapore, 1983.

W.Sierpiński, Elementary theory of numbers, Warszawa-Amsterdam-New York-Oxford 1987.

Z.I. Borevich, I.R.Shafarevich, Number Theory, Academic Press 1966

H. Davenport, The Higher Arithmetic, Cambridge University Press.

G. H. Hardy and E. M. Wright, An Introduction to the Theory of Numbers,
Oxford University Press, 1979.

Requirements to pass the lectures and exercises.

General notes regarding the course:

To pass the course, you need to pass the final exam in the end,

and you need to pass the exercises.

Students must score at least 60 percent on the exam to pass.

Requirements to pass the lectures and exercises.

General notes regarding the course:

To pass the exercises you need to pass:

homework exercises (which will be put on the webpage in due course)

and two tests.

Minimum passing is 60 percent.

The maximum number of lessons that a student may

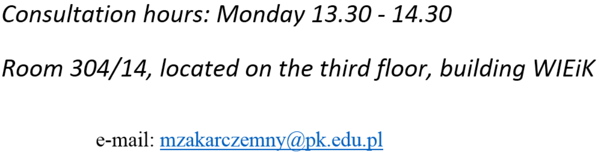
be absent without acceptable documentation justifying the absence is 2.

Class attendance is required of all undergraduates unless the student has

an official excused absence.

Excused absences are granted for one general reason:

Student has a documented personal reason (illness, injury, health condition etc.).



Consultation hours: Monday 13.30 - 14.30

Room 304/14, located on the third floor, building WIEiK

e-mail: mzakarczemny@pk.edu.pl