ELEMENTARY NUMBER THEORY

W W L CHEN

Chapter 1

DIVISION AND FACTORIZATION

1.1. Division

Suppose that $a, b \in \mathbb{Z}$ and $a \neq 0$. Then we say that a divides b, denoted by $a \mid b$, if there exists $c \in \mathbb{Z}$ such that $b = ac$. In this case, we also say that a is a divisor of b, or that b is a multiple of a.

THEOREM 1A. *Suppose that $a \in \mathbb{N}$ and $b \in \mathbb{Z}$. Then there exist unique $q, r \in \mathbb{Z}$ such that $b = aq + r$ and $0 \le r < a$.*

Proof. We shall first of all show the existence of such numbers $q, r \in \mathbb{Z}$. Consider the set

$$S = \{b - as \ge 0 : s \in \mathbb{Z}\}.$$

Then it is easy to see that S is a non-empty subset of $\mathbb{N} \cup \{0\}$. It follows from the Principle of induction that S has a smallest element. Let r be the smallest element of S, and let $q \in \mathbb{Z}$ such that $b - aq = r$. Clearly $r \ge 0$, so it remains to show that $r < a$. Suppose on the contrary that $r \ge a$. Then $b - a(q+1) = (b - aq) - a = r - a \ge 0$, so that $b - a(q+1) \in S$. Clearly $b - a(q+1) < r$, contradicting that r is the smallest element of S.

Next we show that such numbers $q, r \in \mathbb{Z}$ are unique. Suppose that

$$b = aq_1 + r_1 = aq_2 + r_2.$$

Then

$$|r_1 - r_2| = a|q_2 - q_1|.$$

If $q_1 \neq q_2$, then it is easy to see that $a|q_2 - q_1| \ge a$, while $|r_1 - r_2| < a$, a contradiction. It follows that $q_1 = q_2$, and so $r_1 = r_2$ also. ◯

We next establish the existence of the greatest common divisor.

THEOREM 1B. *Suppose that $a, b \in \mathbb{N}$. Then there exists a unique $d \in \mathbb{N}$ such that*
(i) there exist $x, y \in \mathbb{Z}$ such that $d = ax + by$;
(ii) $d \mid a$ and $d \mid b$; and
(iii) for every $k \in \mathbb{N}$ such that $k \mid a$ and $k \mid b$, we have $k \mid d$.

PROOF. Consider the set

$$I = \{au + bv : u, v \in \mathbb{Z}\}.$$

Then it is easy to see that I is a non-empty subset of $\mathbb{Z}$ which contains some positive integers. It follows from the Principle of induction that I has a least positive element. Let d be the least positive element of I, and let $x, y \in \mathbb{Z}$ such that $d = ax + by$. The conclusion (i) follows trivially. Also, d is uniquely defined.

Next, we shall show that d divides every integer in I. Suppose that $z = au + bv$ is any given integer in I. By Theorem 1A, there exist $q, r \in \mathbb{Z}$ such that $z = dq + r$, where $0 \le r < d$. Then

$$r = z - dq = a(u - xq) + b(v - yq) \in I.$$

If $r \neq 0$, then the requirement $0 < r < d$ contradicts the minimality of d. Hence $r = 0$, so that $z = dq$, whence d divides z.

Taking $u = 1$ and $v = 0$ gives $d \mid a$. Taking $u = 0$ and $v = 1$ gives $d \mid b$. Also, the conclusion (iii) is a simple consequence of (i). ◯

The number d in Theorem 1B is called the greatest common divisor of a and b, and denoted by $d = (a, b)$. Two numbers $a, b \in \mathbb{N}$ are said to be relatively prime, or coprime, if $(a, b) = 1$.

A practical way of finding the greatest common divisor of two natural numbers is given by the following result.

THEOREM 1C. (EUCLID'S ALGORITHM) *Suppose that $a, b \in \mathbb{N}$, and $a < b$. Suppose further that $q_1, \ldots, q_{n+1} \in \mathbb{Z}$ and $r_1, \ldots, r_n \in \mathbb{N}$ satisfy $0 < r_n < r_{n-1} < \ldots < r_1 < a$ and*

$$\begin{aligned} b &= aq_1 + r_1, \\ a &= r_1 q_2 + r_2, \\ r_1 &= r_2 q_3 + r_3, \\ &\;\;\vdots \\ r_{n-2} &= r_{n-1} q_n + r_n, \\ r_{n-1} &= r_n q_{n+1}. \end{aligned}$$

Then $(a, b) = r_n$.

PROOF. We shall first of all prove that

$$(a, b) = (a, r_1). \tag{1}$$

Note that we have $(a, b) \mid a$ and $(a, b) \mid (b - aq_1) = r_1$, and so

$$(a, b) \mid (a, r_1).$$

On the other hand, we have $(a, r_1) \mid a$ and $(a, r_1) \mid (aq_1 + r_1) = b$, and so

$$(a, r_1) \mid (a, b).$$

Equality (1) follows. Similarly

(2) $$(a, r_1) = (r_1, r_2) = (r_2, r_3) = \ldots = (r_{n-1}, r_n).$$

Note now that

(3) $$(r_{n-1}, r_n) = (r_n q_{n+1}, r_n) = r_n.$$

The result follows on combining (1)–(3). ◯

EXAMPLE. Consider $(589, 5111)$. In our notation, we let $a = 589$ and $b = 5111$. Then we have

$$\begin{aligned} 5111 &= 589 \cdot 8 + 399, \\ 589 &= 399 \cdot 1 + 190, \\ 399 &= 190 \cdot 2 + 19, \\ 190 &= 19 \cdot 10. \end{aligned}$$

It follows that $(589, 5111) = 19$. On the other hand,

$$\begin{aligned} 19 &= 399 - 190 \cdot 2 \\ &= 399 - (589 - 399 \cdot 1) \cdot 2 \\ &= 589 \cdot (-2) + 399 \cdot 3 \\ &= 589 \cdot (-2) + (5111 - 589 \cdot 8) \cdot 3 \\ &= 5111 \cdot 3 + 589 \cdot (-26). \end{aligned}$$

It follows that $x = -26$ and $y = 3$ satisfy $589x + 5111y = (589, 5111)$.

A very useful result concerning divisors is the following.

THEOREM 1D. *Suppose that $a, b \in \mathbb{N}$ and $(a, b) = 1$. Suppose further that $w \in \mathbb{N}$ satisfies $w \mid ab$. Then there exist unique $u, v \in \mathbb{N}$ such that $u \mid a$, $v \mid b$ and $w = uv$.*

PROOF. We shall first of all show that $u = (w, a)$ and $v = (w, b)$ satisfy the requirements. Consider the number $(w, a)(w, b)$. By Theorem 1B, there exist $x_1, y_1, x_2, y_2 \in \mathbb{Z}$ such that $(w, a) = wx_1 + ay_1$ and $(w, b) = wx_2 + by_2$, so that

$$(w, a)(w, b) = (wx_1 + ay_1)(wx_2 + by_2) = w(wx_1x_2 + ay_1x_2 + bx_1y_2) + aby_1y_2.$$

It follows that

(4) $$w \mid (w, a)(w, b).$$

On the other hand, since $(a, b) = 1$, it follows from Theorem 1B that there exist $x, y \in \mathbb{Z}$ such that $ax + by = 1$, so that $w = wax + wby$. Note now that $(w, a) \mid a$ and $(w, b) \mid w$, so that $(w, a)(w, b) \mid wax$. Note also that $(w, a) \mid w$ and $(w, b) \mid b$, so that $(w, a)(w, b) \mid wby$. It follows that

(5) $$(w, a)(w, b) \mid w.$$

Combining (4) and (5), and noting that $w, (w, a), (w, b) \in \mathbb{N}$, we conclude that $w = (w, a)(w, b)$.

To show uniqueness, it suffices to show that if $u, v \in \mathbb{N}$ satisfy $u \mid a$, $v \mid b$ and $w = uv$, then $u = (w, a)$ and $v = (w, b)$. Since $u \mid w$ and $u \mid a$, it follows from Theorem 1B that $u \mid (w, a)$. Similarly $v \mid (w, b)$. Suppose on the contrary that $u \neq (w, a)$. Then $u < (w, a)$, so that $w = uv < (w, a)(w, b) = w$, a contradiction. A similar contradiction arises if $v \neq (w, b)$. ◯

1.2. Factorization

Suppose that $a \in \mathbb{N}$ and $a > 1$. Then we say that a is prime if it has exactly two positive divisors, namely 1 and a. We also say that a is composite if it is not prime. It is convenient to treat the integer 1 as neither prime nor composite. To find a good reason for not including 1 as a prime, see the Remark following Theorem 1G.

Throughout these notes, the symbol p, with or without suffices, denotes a (positive) prime.

THEOREM 1E. *Suppose that $a, b \in \mathbb{Z}$, and p is a prime. If $p \mid ab$, then $p \mid a$ or $p \mid b$.*

PROOF. Suppose that $p \nmid a$. Since p is prime, the only positive divisors of p are 1 and p. Hence we must have $(a, p) = 1$. It follows from Theorem 1B that there exist $x, y \in \mathbb{Z}$ such that $1 = ax + py$, so that $b = abx + pby$. Clearly $p \mid b$. ◯

Using Theorem 1E a finite number of times, we have the following generalization.

THEOREM 1F. *Suppose that $a_1, \ldots, a_k \in \mathbb{Z}$, and p is a prime. If $p \mid a_1 \ldots a_k$, then $p \mid a_j$ for some $j = 1, \ldots, k$.*

THEOREM 1G. (FUNDAMENTAL THEOREM OF ARITHMETIC) *Every natural number $n > 1$ is representable as a product of primes, uniquely up to the order of factors.*

REMARK. If the integer 1 were included as a prime, then we would have to rephrase the statement of the Fundamental theorem of arithmetic to allow for different representations like $6 = 2 \cdot 3 = 1 \cdot 2 \cdot 3$.

PROOF OF THEOREM 1G. We shall first of all show by induction that every integer $n \geq 2$ is representable as a product of primes. Clearly 2 is a product of primes. Assume now that $n > 2$ and that every $m \in \mathbb{N}$ satisfying $2 \leq m < n$ is representable as a product of primes. If n is a prime, then it is obviously representable as a product of primes. If n is not a prime, then there exist $n_1, n_2 \in \mathbb{N}$ satisfying $2 \leq n_1 < n$ and $2 \leq n_2 < n$ such that $n = n_1 n_2$. By our induction hypothesis, both n_1 and n_2 are representable as products of primes, so that n must also be representable as a product of primes.

Next we shall show uniqueness. Suppose that

$$n = p_1 \ldots p_r = p'_1 \ldots p'_s, \tag{6}$$

where $p_1 \leq \ldots \leq p_r$ and $p'_1 \leq \ldots \leq p'_s$ are primes. Now $p_1 \mid p'_1 \ldots p'_s$, so it follows from Theorem 1F that $p_1 \mid p'_j$ for some $j = 1, \ldots, s$. Since p_1 and p'_j are both primes, we must then have $p_1 = p'_j$. On the other hand, $p'_1 \mid p_1 \ldots p_r$, so again it follows from Theorem 1F that $p'_1 \mid p_i$ for some $i = 1, \ldots, r$, so again we must have $p'_1 = p_i$. It now follows that $p_1 = p'_j \geq p'_1 = p_i \geq p_1$, so that $p_1 = p'_1$. Removing the factor $p_1 = p'_1$ from (1), we obtain

$$p_2 \ldots p_r = p'_2 \ldots p'_s.$$

Repeating this argument a finite number of times, we conclude that $r = s$ and $p_i = p'_i$ for every $i = 1, \ldots, r$. ◯

Grouping together equal primes, we can reformulate Theorem 1G as follows.

THEOREM 1H. *Every natural number $n > 1$ is representable uniquely in the form*

$$n = p_1^{m_1} \ldots p_r^{m_r}, \tag{7}$$

where $p_1 < \ldots < p_r$ are primes, and where $m_j \in \mathbb{N}$ for every $j = 1, \ldots, r$.

The representation (7) is called the canonical decomposition of the natural number n.

1.3. Some Elementary Properties of Primes

There are many consequences of the Fundamental theorem of arithmetic. The following is one which concerns primes.

THEOREM 1J. (EUCLID) *There are infinitely many primes.*

PROOF. Suppose on the contrary that $p_1 < \ldots < p_r$ are all the primes. Let

$$n = p_1 \ldots p_r + 1.$$

Then $n \in \mathbb{N}$ and $n > 1$. It follows from the Fundamental theorem of arithmetic that $p_j \mid n$ for some $j = 1, \ldots, r$, so that $p_j \mid (n - p_1 \ldots p_r) = 1$, a contradiction. ○

Let p be a prime. For any given $n \in \mathbb{N}$, it is an interesting problem to find the largest integer k such that $p^k \mid n!$. In order to describe the answer to this question, we need to define one of the most useful functions in number theory.

Suppose that $\alpha \in \mathbb{R}$. The number $[\alpha] \in \mathbb{Z}$ is defined to be the unique integer $m \in \mathbb{Z}$ satisfying $m \le \alpha < m + 1$. We call $[\alpha]$ the integer part of α.

EXAMPLES. We have $[\pi] = 3$, $[5] = 5$ and $[-\pi] = -4$.

The integer part function has many interesting properties. The proof of the following results is left as an exercise.

REMARKS. Suppose that $\alpha, \beta \in \mathbb{R}$.

(i) We have $\alpha - 1 < [\alpha] \le \alpha$ and $0 \le \alpha - [\alpha] < 1$.

(ii) If $\alpha \ge 0$, then $[\alpha]$ counts the number of natural numbers not exceeding α. In other words,

$$[\alpha] = \sum_{1 \le n \le \alpha} 1.$$

(iii) For every $n \in \mathbb{Z}$, we have $[\alpha + n] = [\alpha] + n$.

(iv) We have $[\alpha] + [\beta] \le [\alpha + \beta] \le [\alpha] + [\beta] + 1$.

(v) If $\alpha \in \mathbb{Z}$, then $[\alpha] + [-\alpha] = 0$. If $\alpha \notin \mathbb{Z}$, then $[\alpha] + [-\alpha] = -1$.

(vi) The number $-[-\alpha]$ is the smallest integer not less than α.

(vii) If $n \in \mathbb{N}$, then $[[\alpha]/n] = [\alpha/n]$.

(viii) The number $[\alpha+1/2]$ is one of the two nearest integers to α. Furthermore, if these two integers both differ from α by the same value, then $[\alpha + 1/2]$ is the larger of these two integers.

(ix) If $\alpha > 0$ and $n \in \mathbb{N}$, then $[\alpha/n]$ is the number of positive integers not exceeding α and which are multiples of n.

THEOREM 1K. *Suppose that $n \in \mathbb{N}$ and p is a prime. Then the largest integer k such that $p^k \mid n!$ is given by*

$$k = \sum_{j=1}^{\infty} \left[\frac{n}{p^j} \right].$$

Proof. Suppose that $m \in \mathbb{N}$ and $1 \le m \le n$. If $p^r \mid m$ and $p^{r+1} \nmid m$, we want to count a contribution of r. In other words, we count a contribution of 1 for every $j \in \mathbb{N}$ such that $p^j \mid m$. Hence

$$k = \sum_{m=1}^{n} \sum_{\substack{j=1 \\ p^j \mid m}}^{\infty} 1 = \sum_{j=1}^{\infty} \sum_{\substack{m=1 \\ p^j \mid m}}^{n} 1 = \sum_{j=1}^{\infty} \left[\frac{n}{p^j} \right],$$

in view of Remark (ix) above. ◯

If $m \in \mathbb{N}$ and p is prime, we sometimes write $p^r \parallel m$ if $p^r \mid m$ and $p^{r+1} \nmid m$.

Example. Suppose that $3^k \parallel 150!$. Then

$$\begin{aligned} k &= \left[\frac{150}{3}\right] + \left[\frac{150}{3^2}\right] + \left[\frac{150}{3^3}\right] + \left[\frac{150}{3^4}\right] + \left[\frac{150}{3^5}\right] + \ldots \\ &= 50 + 16 + 5 + 1 + 0 + \ldots \\ &= 72. \end{aligned}$$

1.4. Some Results and Problems Concerning Primes

Given that there are infinitely many primes, a natural question that arises is to determine the number $\pi(X)$ of primes that do not exceed a given real number X. This was the subject of much investigation in the 1800's. For example, Legendre proposed in 1808 that there is a constant A such that for large values of X, the number $\pi(X)$ can be approximated by

$$\frac{X}{\log X - A}. \tag{8}$$

Gauss proposed the function

$$\frac{1}{\log x}$$

as an approximation to the average density of distribution of primes near any large real number x, and thus formulated the function

$$\int_2^X \frac{\mathrm{d}x}{\log x} \tag{9}$$

as an approximation to $\pi(X)$. Note that the dominating term in the integral is

$$\frac{X}{\log X}, \tag{10}$$

so perhaps

$$\lim_{X \to \infty} \frac{\pi(X) \log X}{X} = 1. \tag{11}$$

Indeed, Tchebycheff showed in 1848 that if the limit in (11) exists at all, then it must be equal to 1. Unfortunately, he and others were unable to show that the limit exists. Then in 1850, he showed that there exist positive constants c_1 and c_2 such that for every real number $X \ge 2$, we have

$$c_1 \frac{X}{\log X} < \pi(X) < c_2 \frac{X}{\log X}.$$

This confirms that the function (10) at least represents the correct order of magnitude of $\pi(X)$. We shall prove Tchebycheff's theorem in Chapter 6.

The crucial idea that finally led to the proof of (11) was introduced by Riemann in a monumental contribution in 1860. Riemann observed that the series

$$\sum_{n=1}^{\infty} \frac{1}{n^s} \tag{12}$$

plays a crucial role in the study of the distribution of primes if one treats s as a complex variable. It follows that the distribution of primes can be studied by the use of methods in the theory of analytic functions. Riemann denoted the series (12) by $\zeta(s)$, and the function has since been known as the Riemann zeta function. Indeed, Riemann's work has also influenced greatly the development of the general theory of functions.

Riemann's ideas were studied in great depth in the late 1800's by von Mangoldt and Hadamard. This culminated in the proof of (11) in 1896 by Hadamard and de la Vallée Poussin, independently and almost simultaneously. In particular, the work of de la Vallée Poussin showed that the integral (9) is a better approximation to $\pi(X)$ than the function (8) for any value of the constant A.

The result (11) is known nowadays as the Prime number theorem.

Problems for Chapter 1

1. Suppose that $a, b, c \in \mathbb{N}$. Prove each of the following:
   (i) If $a \mid b$ and $b \mid c$, then $a \mid c$.
   (ii) If $a \mid b$ and $a \mid c$, then $a \mid (bx + cy)$ for every $x, y \in \mathbb{Z}$.

2. Prove that if $n \in \mathbb{N}$ is composite, then it has a prime factor not exceeding $\sqrt{n}$.

3. Prove that $n^4 + 4$ is composite for every natural number $n > 1$.

4. Prove that the three natural numbers $n, n + 2, n + 4$ cannot be simultaneously prime unless $n = 3$.

5. Suppose that $p > 3$ is a prime.
   (i) Explain why $p = 6k + 1$ or $p = 6k - 1$ for some $k \in \mathbb{N}$.
   (ii) Use this to show that $24 \mid (p^2 - 1)$.

6. Prove that $24 \mid n(n^2 - 1)$ for every odd $n \in \mathbb{N}$.

7. Prove that for every natural number $n > 2$, at least one of $2^n - 1$ and $2^n + 1$ is composite.

8. Suppose that $a, b, c \in \mathbb{N}$.
   (i) Prove that if $3 \mid (a^2 + b^2)$, then $3 \mid ab$.
   (ii) Prove that if $9 \mid (a^3 + b^3 + c^3)$, then $3 \mid abc$.

9. Suppose that $m, n \in \mathbb{N}$.
   (i) Prove that $n! \mid (m + 1)(m + 2) \ldots (m + n)$.
   (ii) Prove that $6 \mid (n^3 - n)$ and $120 \mid (n^5 - 5n^3 + 4n)$.
   (iii) Prove that $\dfrac{(3m)!(4n)!}{(m!)^3(n!)^4} \in \mathbb{N}$.

10. Suppose that $n_1, \ldots, n_k \in \mathbb{N}$. Prove that $n_1! \ldots n_k!$ divides $(n_1 + \ldots + n_k)!$.

11. Suppose that p is a prime.
   (i) Prove that $\binom{p}{k}$ is divisible by p for every $k = 1, 2, \ldots, p-1$.
   (ii) Prove that $2^p - 2$ is divisible by p.

12. Suppose that $n \in \mathbb{N}$ and $2^n + 1$ is prime. Prove that n is a power of 2.

13. The Fermat numbers F_n are defined by $F_n = 2^{2^n} + 1$ for every non-negative integer n.
   (i) Prove that for every $k \in \mathbb{N}$, we have $F_n \mid (F_{n+k} - 2)$.
   (ii) Deduce that the Fermat numbers are pairwise coprime.
   (iii) Explain why this implies that there are infinitely many primes.

14. A rational number a/b with $(a, b) = 1$ is called a reduced fraction. If a sum of two reduced fractions is an integer, say $(a/b) + (c/d) \in \mathbb{Z}$, prove that $|b| = |d|$.

15. Suppose that $a, b, c, d \in \mathbb{N}$. Prove each of the following without using prime factorizations:
   (i) If $a \mid bc$ and $(a, b) = 1$, then $a \mid c$.
   (ii) $(a, b) = d$ if and only if $(a/d, b/d) = 1$.
   (iii) $(ac, bc) = c(a, b)$.
   (iv) $(a, bc) = (a, (a, b)c)$.
   (v) $(a^2, b^2) = (a, b)^2$.

16. Suppose that $a, b, c, d, x, y \in \mathbb{N}$, where $ad - bc = \pm 1$. Prove that if $m = ax + by$ and $n = cx + dy$, then $(m, n) = (x, y)$.

17. Suppose that $a, b \in \mathbb{N}$.
   (i) Prove that there exists a unique $m \in \mathbb{N}$ such that
      - $a \mid m$ and $b \mid m$; and
      - if $x \in \mathbb{N}$ satisfies $a \mid x$ and $b \mid x$, then $m \mid x$.
   (ii) We write $m = [a, b]$ and call it the least common multiple of a and b. Describe $[a, b]$ in terms of canonical decompositions.

18. Suppose that $a, b, c \in \mathbb{N}$.
   (i) Describe the greatest common divisor (a, b, c) and the least common multiple $[a, b, c]$ in terms of canonical decompositions.
   (ii) Show that $\dfrac{[a, b, c]^2}{[a, b][a, c][b, c]} = \dfrac{(a, b, c)^2}{(a, b)(a, c)(b, c)}$.

19. Suppose that $a, m, n \in \mathbb{N}$ and $a \neq 1$. Prove that $(a^m - 1, a^n - 1) = a^{(m,n)} - 1$.

20. Find $(589, 5111)$. Find also integers x and y such that $(589, 5111) = 589x + 5111y$. Hence give the general solution of this equation in integers x and y.

21. Prove that there are infinitely many primes of the form $4n - 1$.

22. Prove that $\left[\dfrac{m+n}{2}\right] + \left[\dfrac{n-m+1}{2}\right] = n$ for every $m, n \in \mathbb{Z}$.

23. Suppose that $a, b \in \mathbb{N}$ satisfy $(a, b) = 1$. Prove that

$$\sum_{k=1}^{a-1} \left[\frac{kb}{a}\right] = \sum_{\ell=1}^{b-1} \left[\frac{\ell a}{b}\right] = \frac{(a-1)(b-1)}{2}$$

   by considering the open rectangle with vertices at $(0, 0)$, $(a, 0)$, $(0, b)$ and (a, b), split into two halves by the line segment $ay = bx$ where $0 < x < a$. Show first that there are no lattice points $(m, n) \in \mathbb{N}^2$ on the line segment between the endpoints $(0, 0)$ and (a, b). Then count lattice points $(m, n) \in \mathbb{N}^2$ in one of the two open triangular regions.

24. Suppose that $n \in \mathbb{N}$, and that $\alpha \in \mathbb{R}$ is non-negative. Prove Hermite's identity, that

$$\sum_{k=0}^{n-1} \left[\alpha + \frac{k}{n}\right] = [n\alpha].$$

25. Suppose that $n \in \mathbb{N}$. Prove that

$$\sum_{k=0}^{\infty} \left[\frac{n+2^k}{2^{k+1}}\right] = n$$

by using the binary digit expansion

$$n = \sum_{m=0}^{\infty} a_m 2^m, \qquad \text{where } a_0, a_1, a_2 \ldots \in \{0,1\},$$

noting that $a_m \neq 0$ for finitely many non-negative integers m.

26. Prove that $2^n \mid (n+1)(n+2)\ldots(2n)$ for every $n \in \mathbb{N}$.

27. With how many zeros does the decimal digit expansion of 2003! end?

28. Find the largest two-digit prime factor of $\binom{200}{100}$.

29. Suppose $n \in \mathbb{N}$, and that $p \geq \sqrt{2n}$ is a prime such that p divides $\binom{2n}{n}$. Prove that p^2 does not divide $\binom{2n}{n}$.