4.3 Euclidean Number Theory

Books VII, VIII and IX of the Elements were on Number Theory. Two major results are:

Proposition 14 which says that every integer greater or equal 2 can be factored as a product of prime numbers in one and only one way.

Proposition 20 which says there are infinitely many prime numbers.

We start with some elementary definitions and results to give a flavor of this work.

Definition: We say a divides b or b is divisible by a and write $a|b$ if a and b are integers $a \neq 0$ and there is an integer k so that $b = ka$. If a does not divide b then we write $a \nmid b$.

Observe here that we can now allow negative integers in our discussion even if Euclid would not.

Example; $13|52$ but $39 \nmid 52$.

There is a list of the properties of this relation on page 165.

1. For any integer a, $a|0$, $1|a$ and $a|a$

2.

3.

4. If $a|b$ and $b|c$ then $a|c$.

5. If $a|b$ and $b|a$ then $a = \pm b$.

6. If $a|b$ and $a|c$ then $a|xb + yc$ for any integers x and y

Property 6 is verfied in the book. Property 4 could be verified as follows: If $a|b$ and $b|c$ then $a \neq 0$ and $b = ka$ and $c = lb$ for some integers k and l. Therefore $c = lka$ so that $a|c$.

The set of all positive divisors of 24 are $\{1, 2, 3, 4, 6, 8, 12, 24\}$. Observe that 1 and 24 are included.

Definition: An integer $p > 1$ is a *prime* if its only positive divisors are 1 and p. An integer $n \geq 2$ is *composite* if it is not prime.

Therefore if n is composite there exist integers $a \neq 1$ and $b \neq 1$ so that $n = ab$.

List the first 12 primes: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31.

Definition: If a and b are two integers then an integer d is said to be a *common divisor* of a and b if $d|a$ and $d|b$.

13 is a common divisor of 52 and 39. 1 is a common divisor of every pair of integers. Given any integer $a \neq 0$ the set of divisors is finite. We need only check that the set of positive divisors because $a|b$ if and only if $-a|b$. The check goes as follows: every positive divisor d of a satisfies $d \leq |a|$ because if $d > |a| > 0$ then $kd > |a|$ for all integers $k \neq 0$. It follows that the set of common divisors of a and b is a finite set that contains 1.

Definition: The largest of the common divisors of integers $a \neq 0$ and $b \neq 0$ is called the *greatest common divisor* of a and b and is written $\gcd(a, b)$.

Therefore $\gcd(a, b) \geq 1$.

Example: gcd(60,24) = 12.

Division Theorem *For integers a and b there exist unique integers q and r, $0 \leq r < b$ so that*

$$a = qb + r$$

The Euclidean Algorithm: Given integers a and b it is possible to find the greatest common divisor gcd(a,b) as follows

$$\begin{aligned} a &= q_1 b + r_1 \quad 0 \leq r_1 < b \\ b &= q_2 r_1 + r_2 \quad 0 \leq r_2 < r_1 \\ r_1 &= q_2 r_2 + r_3 \quad 0 \leq r_3 < r_2 \\ &\vdots \\ r_{n-2} &= q_{n-1} r_{n-1} + r_n \quad 0 \leq r_n < r_{n-1} \\ r_{n-1} &= q_n r_n + 0 \end{aligned}$$

Then r_n =gcd(a,b)

Example: Find gcd(14456,6864).

$$\begin{aligned} 14456 &= 2(6864) + 728 \\ 6864 &= 9(728) + 312 \\ 728 &= 2(312) + 104 \\ 312 &= 3(104) \end{aligned}$$

so that 104 = gcd(14456,6864).

Return now to the algorithm. Observe that $r_n | r_{n-1}$ and therefore $r_n | r_{n-2}$ and so on until we see r_n divides a and b This proves that r_n is a divisor of a and b. Conversely suppose that k divides a and b. Then k divides r_1 and therefore r_2 and so on so that k divides r_n. If we choose k =gcd(a,b) then we see that gcd(a,b) divides r_n and so r_n = gcd(a,b).

Theorem: *For any integers $a \neq 0$ $b \neq 0$, there exist integers x and y so that*

$$\gcd(a, b) = xa + yb$$

Proof: Check that $r_1 = x_1 a + y_1 b$ for some integers x_1 and y_1 and $r_2 = x_2 a + y_2 b$ and so on so that $r_n = x_n a + y_n b$.

Example: We can express gcd(14456,6864)=104 as follows. Recall the calculation above

$$\begin{aligned} 14456 &= 2(6864) + 728 \\ 6864 &= 9(728) + 312 \\ 728 &= 2(312) + 104 \\ 312 &= 3(104) \end{aligned}$$

and so

$$\begin{aligned} 104 &= 728 - 2(312) = 728 - 2(6864 - 9(728)) = 19(728) - 2(6864) \\ &= 19(14456 - 2(6864)) - 2(6864) = 19(14456) - 40(6864) \end{aligned}$$

Definition: If $a \neq 0$ and $b \neq 0$ are two integers and gcd(a,b) = 1 then a and b are said to be relatively prime.

It follows form our theorem that

Theorem: *If $a \neq 0$ and $b \neq 0$ are two integers then gcd(a,b) = 1 if and only if there exist integers x and y so that $xa + yb = 1$.*

Proof: The existence of x and y was verified in the theorem. Conversely if $xa+yb = 1$ and if d is a common divisor of a and b then $d|(xa + yb)$ so that $d|1$ which means that $d = \pm 1$ and so gcd(a,b) = 1.

Corollary: *If $a \neq 0$ and $b \neq 0$ are two integers and gcd(a,b) = d then gcd(a/d,b/d)=1.*

Proof: By the theorem $xa + yb = d$. Divide by d and apply the Corollary.

Corollary 2: *If $a \neq 0$ and $b \neq 0$ are two integers and gcd(a,b)=1 and if $a|c$ and $b|c$ the $ab|c$.*

Proof: By the Corollary $xa + yb = 1$ for some integers x and y. Therefore $c = c \cdot 1 = cxa + cyb$. On the other hand $c = ra$ and $c = sb$ for some integers r and s so that $c = sbxa + rayb = ab(sx + ry)$ so that $ab|c$

Observe that $12|24$ and $8|24$ but $12 \cdot 8 = 96 \nmid 24$.

Euclid's Lemma: *If $a \neq 0$, $b \neq 0$ and c are integers and $a|bc$ and gcd(a,b) =1 then $a|c$.*

Proof: We have by our theorem $1 = ax + by$ and we further know that $bc = sa$ and so $c = c \cdot 1 = cax + cby = cax + say = a(cx + sy)$ which says $a|c$.

Theorem: *If p is a prime and $p|a_1a_2 \ldots a_n$ then $p|a_k$ for some k.*

Proof: We may assume that $a_j \neq 0$ for each j, $1 \leq j \leq n$. We have gcd(p,a_j) is 1 or p. Taking $j = 1$ we see either $p|a_1$ or gcd(p,a_j)=1 and we can assume the latter and so the previous Lemma applies and we conclude $p|a_2a_3 \ldots a_n$. Repeat the process and finally we conclude if p does not divide a_j $1 \leq j \leq n - 1$ then $p|a_n$.

The Fundamental Theorem of Arithmetic: *Every integer $n \geq 2$ can be written as a product of prime numbers and this representation is unique up to order of the prime factors.*

For example $12 = 2^2 3$. Primes may be repeated.

Proof: We show $n = p_1p_2 \ldots p_k$. If n is prime then we are done ($k = 1$). Otherwise n is composite and so n has a divisor. Let p_1 be the smallest of those divisors. Then p_1 is prime or it is composite $p_1 = ab$ but $1 < a < p_1$ and $a|n$ and this contradicts the choice of p_1. We have $n = p_1n_1$ with $1 < n_1 < n$. If n_1 is prime then we are done ($k = 2$) but if not then it is composite and we can apply the above reasoning to show $n_1 = p_2n_2$ where p_2 is a prime and $1 < n_2 < n_1$ so that $n = p_1p_2n_2$. The process continues with $n > n_1 > n_2 > \ldots$. Eventually we must get to n_k is prime. This proves that there is a prime decomposition.

Now we check uniqueness. Suppose we have two prime decompositions of one number

$$p_1p_2 \ldots p_k = q_1q_2 \ldots q_\ell$$

We may suppose that $p_1 \leq p_2 \leq \ldots p_k$ and $q_1 \leq q_2 \leq \ldots q_\ell$. We may also suppose that all of the p_i are different from all of the q_j because if a prime appeared on both sides of the equation then we could cancel it. Since $p_1|q_1q_2\ldots q_\ell$ we know $p_1|q_j$ for some j by our theorem. But q_j only has positive factors 1 and q_j and so $p_1 = q_j$ but we said that we had already concelled common factors and so this is a contradiction. □

Example: Find the prime decomposition of 1341. Divisible by 3: $1341 = 3(447) = 3^2149$.

Problem 25, page 176: If p is prime then $\sqrt{p}$ is irrational.

Next is Euclid's Proposition 20,

Theorem: *There are infinitely many primes*

Proof: Let p be any prime number. Consider the number $n = p! + 1$. It is not divisible by p or in fact by any prime $q \leq p$ because $n/q = p!/q + 1/q$ and $1/q$ can't be an integer. But n has a prime decomposition and so that must consist entirely of prime numbers larger than p. This shows that given a prime p there exists a larger prime.

4.4 Eratosthenes: Eratosthenes (276-194 B.C.) of Cyrene served as chief librarion at the Library of Alexandria. He was accomplished in many fields but particularly math and geography. His world map is the first to include meridians of longitude and parallels of latitude.

He designed the *mesolabium* to double the cube. It consists of two parallel line AP and FQ that act as slides for three rectangular plates that are indicated in the picture on page 177 by their diagonals. These plates can slide over each other. We suppose that the distance between the two lines is $2a$ where a is the side length of the cube to be doubled. Start from the position on page 177 where the plates are edge to edge and a inclined line is drawn from the upper lefthand corner of the leftmost (fixed) plate to halfway down right edge of the rightmost (third) plate. The three plates are pushed together, the third sliding under the second under the fixed first until the diagonal of the third plate meets the right edge of the second plate and the inclined line and the diagonal of the second meets the right edge of the first and the slant line. This gives us the figure on page 178 if we extend the inclined line AD to meet FQ at E.

To show that x as labelled doubles the cube follow the similar triangles.

$$\frac{x}{a} = \frac{HE}{IE} = \frac{BE}{CE} = \frac{y}{x} = \frac{GE}{HE} = \frac{AE}{BE} = \frac{2a}{y}$$

This is just what Hippocrates of Chios (460-380 B.C.) showed would double the cube because $x^2 = ay$ and $y^2 = 2ax$ so that $x^4 = a^2y^2 = 2a^3x$ or $x^3 = 2a^3$.

The Sieve of Eratosthenes Find all primes less than a given number. Suppose our given number is 40 (the book does 100). Then 2 is one such prime and all other multiples of 2 (even numbers less than 40) can be eliminated. Next comes 3 and all multiples (odd multiples will do) less than 40 can be eliminated and then 5. When we get to 7, we have already eliminated $14 = 7 \cdot 2$, $21 = 7 \cdot 3$ and $28 = 7 \cdot 4$ and $35 = 7 \cdot 5$. Similarly multiples of 11 have already been eliminated. and so what remains is primes. The point is that you only need to cancel the multiples of the primes less of equal $\sqrt{40}$ because if a number less than 40 is composite than one factor is less or equal $\sqrt{40}$. the numbers that are not cancellled are primes.

Problem: Twin Primes If p and $p+2$ are both primes then $(p,p+2)$ is a pair of twin primes. Find 6 twin prime pairs. Are there infinitely many?

The Circumference of the Earth: Eratosthenes and many other educated Greeks knew that the Earth was round. He also knew that on the summer solstice, the sun was directly overhead at Syene (Aswan today) because at noon the sun would shine directly down a deep well. In Alexandria which was 5000 stadia (1 stadia is 516.73 feet) directly north (or so Eratosthenes thought) a shadow made a 7.5 degree angle with a plumb line. Therefore (picture page 180)

$$\frac{\text{circumference}}{360} = \frac{5000}{7.5}$$

from which Eratosthenes gets 252,000 stadia for the circumference. That corresponds (possibly) to 24,662 mile circumference when 24,907 miles is the accepted value today.

Claudius Ptolemy 100-170 A.D. Read about his *Geographike Syntaxis* (which Columbus used) and more importantly his *Almagest* which introduced the theory of epicycles to explain the motion of the planets around the stationary earth.

4.4 Archimedes: Archimedes (287-212 B.C.) of Syracuse probably was visited Alexandria as a young man possibly for his education. He was a favorite of King Hieron II who ruled Syracuse from 269-215 B.C. This was the early period of the expanding Roman Empire and the Punic Wars, (Second Punic War 218-201 B.C.) between Rome and Carthage.

Archimedes was an inventor. One of his inventions, the Archimedean screw is still in use in Egypt today. King Hieron also asked for and got help defending Syracuse from the occasional attack. Archimedes invented instruments of war for the defense of the city such as catapults and a parabolic mirror. However Archimedes was not successful in 212 B.C. Defending King Hieron's son and Syracuse from attack by the Romans. The story often told is that a Roman soldier found Archimedes working on a geometry problem and when he challenged Archimedes who responded with "don't disturb my circles" and the soldier stabbed Archimedes to death.

It is also believed that despite his inventive genius Archimedes most valued his abstract results. For example he showed that a sphere inscribed inside a cylinder has 2/3 the volume of the cylinder and two thirds the surface area (include the ends of the cylinder). He asked that this result be inscribed on his tomb. Maybe it was.

Approximation of π: Recall that π is the ratio of the circumference of a circle to the diameter. If we inscribe or circumscribe polygons in a circle of radius 1 and measure their perimeter we should get an approximation of 2π. This is the *method of exhaustion*

(originally due to Eudoxus of Cnidos (390-337 B.C.) but remembered more because of the work of Euclid and Archimedes.

The perimeter p_n of an inscribed polygon with n sides is clearly less than 2π. If we double the number of sides then we increase the perimeter (Picture page 193). $p_n \leq p_{2n} \leq 2\pi$

As for the circumscribed polygons, they have perimeter P_n if there are n sides and it is straightforward to see that $P_{2n} < P_n$ because the $2n$-gon can be constructed from the n-gon by cutting off corners. It is perhaps more difficult to see that $P_n > 2\pi$. Think of unwrapping a piece of thread from around the circle.

In the end we get

$$p_n < p_{2n} < p_{4n} < p_{8n} < \ldots < 2\pi < \ldots P_{8n} < P_{4n} < P_{2n} < P_n$$

Not surprisingly we can take a limit and squeeze 2π: $\lim_{k\to\infty} p_{2^k n} = \lim_{k\to\infty} P_{2^k n}$. We can verify all these steps more easily if we use trigonometry (which didn't emerge for about 1300 years). Since an n-gon's side subtends an angle of $2\pi/n$

$$p_n = 2n \sin\left(\frac{\pi}{n}\right) \qquad \text{and} \qquad P_n = 2n \tan\left(\frac{\pi}{n}\right)$$

We can then show that the following recursion relations hold

$$P_{2n} = \frac{2p_n P_n}{p_n + P_n}$$

which says P_{2n} is the harmonic mean of P_n and p_n. Also

$$p_{2n} = \sqrt{p_n P_{2n}}$$

We know $p_6 = 6$ and $P_6 = 4\sqrt{3} \approx 6.93$ and these formulas allow us to compute $P_{12} = 24(2 - \sqrt{3}) \approx 6.43$ and then $p_{12} = 12\sqrt{2 - \sqrt{3}} \approx 6.2117$ Of course we are replacing the problem of approximating $\pi \approx 6.283185$ with the problem of approximating square roots but that is comparatively easy. For example $3 \approx 49/16$ so that $\sqrt{3} \approx 7/4$ and we know the tangent line approximation ($\sqrt{a+h} \approx \sqrt{a} + (1/2\sqrt{a})h$) as did Archimedes. Archimedes ended up with the estimate $3 + (10/71)\pi < 3 + (1/7)$.

Archimedes included this in his treatise *The Measurement of the Circle* which also included the following.

Proposition 1: *The area of a circle equals the area of a right triangle with one side equal the radius and the other side equal to the circumference of the circle.*

The *Elements* also contained such a result.

Quadrature of the Parabola: Find the area inside a parabola cut off by a chord. Archimedes used the "method of exhaustion." Picture of $y = x^2$ with two points (a, a^2) and (y, y^2) and the chord they form.

The largest triangle that has base this chord, meets the parabola at the point where the tangent is parallel to the chord, which maximizes the altitude. The slope of the chord is $b+a$ and so the point is $((b+a)/2, (b+a)^2/4)$. The area of the triangle is $(b-a)^3/8$.(!) (Could use Heron's (75 A.D.) formula $\sqrt{s(s-a)(s-b)(s-c)}$, p185.) Now we inscribe two more triangles. One corresponds to the chord through $((a+b)/2, (a+b)^2/4)$ and (a, a^2) and the other to the other chord through $((a+b)/2, (a+b)^2/4)$ and (b, b^2). These new triangles have area one eighth of the original triangle so that the three triangles together have area.

$$\left(\frac{(b-a)^3}{8}\right)\left(1+\frac{1}{4}\right)$$

If we continue to add on triangles we get a total area

$$\left(\frac{(b-a)^3}{8}\right)\left(1+\frac{1}{4}+\frac{1}{16}+\frac{1}{64}\right) = \left(\frac{(b-a)^3}{8}\right)\frac{1}{1-(1/4)} = \frac{4}{3}\left(\frac{(b-a)^3}{8}\right)$$

That is the area is 4/3 times the area of the first inscribed triangle for recall the geometric series:

$$a + ar + ar^2 + \ldots + ar^n = \frac{a(1-r^{n+1})}{1-r}$$

In calculus we compute the same area as

$$\int_a^b (a+b)x - ab - x^2\,dx \left(= \frac{(b-a)^3}{6}\right)$$

Read about the sprial of Archimedes ($r = a\theta$ in polar coordinates) and look at problems 10 and 11 on page 200.