2 Elementary number theory

2.1 Introduction

Elementary number theory is concerned with properties of the integers. Hence we shall be interested in the following sets:

- The set if integers $\{\ldots -2, -1, 0, 1, 2, 3, \ldots\}$, denoted by $\mathbb{Z}$
- The set of natural numbers $\{0, 1, 2, 3 \ldots\}$, denoted by $\mathbb{N}$
- The set of positive integers $\{1, 2, 3, \ldots\}$, denoted by $\mathbb{Z}^+$
- The set of prime numbers $\{2, 3, 5, 7, 11, 13, \ldots\}$, denoted by $\mathbb{P}$

"Elementary number theory" means the part of number theory that does not require heavy background in pure mathematics. But elementary does not mean easy!! There are many extremely hard problems in elementary number theory, for example the following:

Problem 1. Find all solutions to the following equation:

$$a^{(b^2)} = b^a$$

where a and b are positive integers.

This problem can be solved using only some calculus and really basic properties of the integers (such as the Fundamental Theorem of Arithmetic, see below), but it is still a very difficult problem!
In this part of the course, we will prove most of the theorems we state, with the aim of making you familiar with rigorous mathematical proofs. Number theory is a good area for starting to learn about proofs, since most proofs are short and not to hard to understand. However, we will not prove every theorem, because of our limited time, and because I don't want to torment you with proofs that don't give any particular insights. You are expected to:

- Understand and remember the statement of every theorem
- Be able to use the theorems for computations in concrete examples, such as the exercises of section 2.2 and 2.3 below
- For the final exam, be able to prove the theorems that are proved in these printed lecture notes (however, if you only aim for a passing grade, it should not be necessary to know the proofs)

2.2 Division, factorization and prime numbers

Definition 6. Let a and b be integers. If there exists an integer m such that $b = ma$, then we say that a *divides* b, or that a is a *divisor* of b, or that b is a *multiple* of a, or that b is *divisible* by a. We write this as $a|b$.

For example, 5 divides 15, and 6 divides 12. In other words, 15 is a multiple of 5 and 12 is a multiple of 6.

Example 1. List all the positive divisors of 6. Answer: 1, 2, 3, 6.

Example 2. List all the positive divisors of 11. Answer: 1, 11.

Example 3. List all the positive divisors of 32. Answer: 1, 2, 4, 8, 16, 32.

2.2.1 Prime numbers

Definition 7. Let $a > 1$ be an integer. We say that a is a *prime number* if has exactly two positive divisors, namely 1 and a. We say that a is *composite* if it is not prime.

The number 1 is neither prime nor composite.
There is a simple method for listing the prime numbers up to any given size. This method is called Eratosthenes sieve. It goes as follows:

1. Write down the numbers 2, 3, 4, ... as far as you like.
2. Draw a circle around the number 2, and cross out all larger multiples of 2, that is 4, 6, 8, ...
3. Take the smallest untouched number in the list. Draw a circle around it, and cross out all larger multiples of it.
4. Repeat step 3 until you come to the end of the list.
5. Now all the prime numbers have a circle, and the composite numbers are crossed.

If you try this, you will see that the first few prime numbers are

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, \ldots$$

2.2.2 Quotient and remainder

Now let's discuss the concepts of quotient and remainder. You have probably seen this a very long time ago, in primary school. For example, when we divide 17 by 5, the quotient is 3 and the remainder is 2.

Definition 8. Let a, b be positive integers. In the division $\frac{a}{b}$, the *quotient* is the largest number q such that $a \geq bq$. We denote it by q or $q(a, b)$. The *remainder* is the number $(a - bq)$, denoted by r or $r(a, b)$.

Example 4. In the division $\frac{10}{3}$, the quotient is 3, and the remainder is 1. Hence $q(10,3) = 3$ and $r(10,3) = 1$.

Example 5. In the division $\frac{24}{6}$, the quotient is 4, and the remainder is 0. Hence $q(24,6) = 4$ and $r(24,6) = 0$.

Example 6. In the division $\frac{19}{5}$, the quotient is 3, and the remainder is 4.

Example 7. In the division $\frac{1983}{179}$, the quotient is 11, and the remainder is 14.

2.2.3 GCD and LCM

Definition 9. When a and b are integers, not both zero, we write $GCD(a,b)$ for the greatest common divisor of a and b, that is the largest positive integer that divides both a and b. In the case where a and b are both zero, we define $GCD(a,b)$ to be 0.

Example 8. $GCD(15,12) = 3$. $GCD(24,42) = 6$. $GCD(19,28) = 1$.

Example 9. $GCD(-12,-8) = 4$. $GCD(0,35) = 35$. $GCD(-11,0) = 11$.

Definition 10. If $GCD(a,b) = 1$, we say that a and b are *coprime*.

Definition 11. When a and b are nonzero integers, we write $LCM(a,b)$ for the least common positive multiple of a and b, that is the smallest positive number that has both a and b as divisors. If a or b (or both) equal zero, we define $LCM(a,b)$ to be zero.

Example 10. $LCM(6,7) = 42$. $LCM(8,-12) = 24$. $LCM(0,27) = 0$.

The best way of finding the GCD of two numbers is to use Euclid's algorithm.

Algorithm 1 (Euclid's algorithm)**.** Suppose that a and b are positive integers, and that we want to find $GCD(a,b)$. The idea of Euclid's algorithm is to produce a decreasing sequence of positive integers, such that the last nonzero number in the sequence is equal to $GCD(a,b)$. We start with a and b, and then we compute remainders.

1. Let m_1 be the largest of a and b
2. Let m_2 be the smaller of a and b
3. Let $m_3 = r(a,b)$.
4. Continue like this, putting $m_{k+1} = r(m_{k-1}, m_k)$.
5. The last nonzero number in the sequence is $GCD(a,b)$.

Let's do one example:

Example 11. Let's compute $GCD(1806, 3174)$. We get the following sequence:

$$\begin{aligned} m_1 &= 3174 \\ m_2 &= 1806 \\ m_3 &= r(3174, 1806) = 1368 \\ m_4 &= r(1806, 1368) = 438 \\ m_5 &= r(1368, 438) = 54 \\ m_6 &= r(438, 54) = 6 \\ m_7 &= r(54, 6) = 0 \end{aligned}$$

so we get $GCD(1806, 3174) = 6$.

The following formula is useful when computing the LCM of two integers. Since we have a method for finding GCD, we can use it to find LCM.

Theorem 2. For any positive integers a and b, we have

$$GCD(a, b) \cdot LCM(a, b) = a \cdot b$$

Proof. This follows immediately from the alternative way of thinking about GCD and LCM, discussed after the Fundamental Theorem of Arithmetic below. □

Example 12. We want to compute $LCM(1254, 779)$. Using Euclid's algorithm, we find that $GCD(1254, 779) = 19$. From the above theorem, we can compute

$$LCM(1254, 779) = \frac{1254 \cdot 779}{19} = 51414$$

2.2.4 Factorization

Now we'll talk about factorization of integers. You have probably seen before that every composite number can be factored into prime numbers. Some examples:

Example 13. $39 = 3 \cdot 13$

Example 14. $70 = 2 \cdot 5 \cdot 7$

Example 15. $686 = 2 \cdot 7 \cdot 7 \cdot 7$ (we usually write this as $2 \cdot 7^3$)

Example 16. $3762 = 2 \cdot 3^2 \cdot 11 \cdot 19$

There is only one way to factor an integer (up to the order of the factors). This is one of the most important statements of Elementary number theory:

Theorem 3 (Fundamental Theorem of Arithmetic)**.** Every positive integer $n > 1$ can be written in a unique way as a product

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$$

where $p_1 < p_2 < \ldots < p_k$ are primes and e_i is a positive integer for every i.

Proof. The proof uses a method called *induction*. We will introduce this method later, and perhaps also give the proof of this theorem, if we have time. □

More examples:

Example 17. The prime factorization of 24 is $2^3 \cdot 3$.

Example 18. The prime factorization of 744 is $2^3 \cdot 3 \cdot 31$.

Example 19. The prime factorization of 18095 is $5 \cdot 7 \cdot 11 \cdot 47$.

Example 20. The prime factorization of 1862 is $2 \cdot 7^2 \cdot 19$.

Of, course, to find the factorization of large numbers it is most convenient to use a computer. If you feel that factoring integers is boring or meaningless, you may be interested in the following: If you can find the prime factorization of the following integer:

74037563479561712828046796097429573142593188889231289084936232638972765034028266276891996419625117843995894330502127585370118968098286733173273108930900552505116877063299072396380786710086096962537934650563796359

then you will be awarded a sum of US$ 30,000 from a research institute in the USA. Later in the course we will explain why someone would pay so much just for a factorization of a large number.
A natural question is the following: How do we determine whether a given number, for example 109, is prime or not? For large numbers, this is a difficult question, but for small numbers, we can use one of two simple methods. We can use either the Eratosthenes sieve (see above) or we can use the following fact:

Theorem 4. If a positive integer n is composite, then it has a prime factor p such that $p \leq \sqrt{n}$.

Proof. Let p be the smallest prime factor of n. Then we have $n = p \cdot m$ for some positive integer m. The number m can not be equal to 1, because that would imply $n = p$, which contradicts the hypothesis that n is composite. Any prime factor of m is at least as large as p, so we must have $p \leq m$. Hence $p^2 \leq p \cdot m$, that is $p^2 \leq n$, which implies $p \leq \sqrt{n}$. We have proved that the smallest prime factor of n is smaller than or equal to $\sqrt{n}$. □

To check whether a given integer n is prime or not, we could check, for each prime number smaller than n, whether p divides n or not. If no such prime divides p, we could conclude that n is itself prime. Because of the above theorem, it is actually sufficient to only try all prime numbers up to $\sqrt{n}$.

Example 21. Is 109 a prime number or not? To find the answer, we must check if 109 is divisible by some prime number smaller than $\sqrt{109} = 10.44\ldots$. These primes are 2, 3, 5, and 7. Checking shows that none of them divides 109, so the number 109 is a prime number.

Example 22. Is 437 a prime number or not? To find the answer, we must check all primes up to $\sqrt{437} = 20.9\ldots$. None of 2, 3, 5, 7, 11, 13, 17 divides 437, but we find that 19 divides 437, so it is not a prime.

2.2.5 Some basic but useful facts

Let n be a positive integer

- $2|n$ if and only if 2 divides the last digit of n
- $5|n$ if and only if 5 divides the last digit of n
- $3|n$ if and only if 3 divides the sum of the digits of n
- $11|n$ if and only if 11 divides the alternating sum of the digits of n

There are also similar rules for 7 and 13, but they are slightly more complicated, and we will not need them.

Example 23. The number 32109 is not divisible by 2 or 5, since the last digit is 9. It is divisible by 3, because the sum of the digits is 15. It is also divisible by 11, because the alternating sum of the digits is

$$3 - 2 + 1 - 0 + 9 = 11$$

which is of course divisible by 11.

2.2.6 Another way of thinking about GCD and LCM

Let a and b be two positive integers. Consider the set of all primes occurring in the prime factorizations of these two integers. Call these primes $q_1, q_2, \ldots q_n$. Then we have

$$a = q_1^{e_1} \cdots q_n^{e_n}$$

and also

$$b = q_1^{f_1} \cdots q_n^{f_n}$$

for some natural numbers e_i and f_i. Some of these e_i and f_i might be zero, for example e_1 will be zero if q_1 does not occur in the factorization of a.
When will it be the case that a divides b? Using the above notation, it will be the case exactly if $e_i \leq f_i$ for each i. For example, the number $18 = 2 \cdot 3^2$ divides the number $252 = 2^2 \cdot 3^2 \cdot 7$, because each exponent in the factorization of 18 is smaller than or equal to the corresponding exponent in the factorization of 252.
We continue to use the notation introduced above, and we want to find the GCD and LCM of a and b. We define new numbers as follows:

$$\begin{aligned} g_i &= \min(e_i, f_i) \\ m_i &= \max(e_i, f_i) \end{aligned}$$

(this means that m_i is the largest of e_i and f_i, and g_i is the smallest.)
With this notation, we have

$$GCD(a, b) = q_1^{g_1} \cdots q_n^{g_n}$$

and

$$LCM(a, b) = q_1^{m_1} \cdots q_n^{m_n}$$

Some examples will make this clearer.

Example 24. Take $a = 1176 = 2^3 \cdot 3 \cdot 7^2$ and $b = 3276 = 2^2 \cdot 3^2 \cdot 7 \cdot 13$. Then, with the above notation, we have

$$q_1 = 2, \quad q_2 = 3, \quad q_3 = 7, \quad q_4 = 13$$

$$e_1 = 3, \quad e_2 = 1, \quad e_3 = 2, \quad e_4 = 0$$

$$f_1 = 2, \quad f_2 = 2, \quad f_3 = 1, \quad f_4 = 1$$

$$g_1 = 2, \quad g_2 = 1, \quad g_3 = 1, \quad g_4 = 0$$

$$m_1 = 3, \quad m_2 = 2, \quad m_3 = 2, \quad m_4 = 1$$

and we can conclude that

$$GCD(a, b) = 2^2 \cdot 3 \cdot 7 = 84, \qquad LCM(a, b) = 2^3 \cdot 3^2 \cdot 7^2 \cdot 13 = 45864$$

Example 25. Take $a = 875 = 5^3 \cdot 7$ and $b = 6885 = 3^4 \cdot 5 \cdot 17$. Then, with the above notation, we have

$$q_1 = 3, \quad q_2 = 5, \quad q_3 = 7, \quad q_4 = 17$$

$$e_1 = 0, \quad e_2 = 3, \quad e_3 = 1, \quad e_4 = 0$$

$$f_1 = 4, \quad f_2 = 1, \quad f_3 = 0, \quad f_4 = 1$$

$$g_1 = 0, \quad g_2 = 1, \quad g_3 = 0, \quad g_4 = 0$$

$$m_1 = 4, \quad m_2 = 3, \quad m_3 = 1, \quad m_4 = 1$$

and we can conclude that

$$GCD(a, b) = 5, \qquad LCM(a, b) = 3^4 \cdot 5^3 \cdot 7 \cdot 17 = 1204875$$

2.2.7 Exercises

E71 Find the quotient and the remainder in the division $\frac{31}{6}$.
E72 Find the quotient and the remainder in the division $\frac{399}{12}$.
E73 Find the quotient and the remainder in the division $\frac{504}{84}$.
E74 Find the prime factorization of the following integers: 9, 21, 39, 51, 53, 72, 88, 91.
E75 Find the prime factorization of the following integers: 18513, 9288, 103350.
For each of the statements E76 to E95, determine whether it is true or false:
E76 $10|24$
E77 $24|10$
E78 $7|49$
E79 8 is a multiple of 4
E80 11 is a multiple of 33
E81 37 is a multiple of 37
E82 18 divides 6
E83 5 is a divisor of 25
E84 6 is a divisor of 9
E85 $49|7$
E86 106 divides 0
E87 0 divides 106
E88 0 divides 0
E89 1 is a divisor of 12
E90 1 is a multiple of 0
E91 8 is a multiple of 1
E92 0 is a multiple of 1
E93 0 is a multiple of 129
E94 0 is a multiple of 1000
E95 27 is divisible by 9

E96 List the positive divisors of 25.
E97 List the positive divisors of 18.
E98 List the first few positive multiples of 7.
E99 List the first few positive multiples of 23.
E100 List the multiples of 0.
E101 Use Eratosthenes sieve to list all primes smaller than 100. How many are they?
E102 Which of the following numbers are prime: 10, 37, 51, 72, 101, 173, 309, 1002, 10235, 13273.
Compute the following quotients and remainders:
E103 $q(180, 18)$.
E104 $r(180, 18)$.
E105 $q(99, 7)$.
E106 $r(99, 7)$.
E107 $q(846, 19)$.
E108 $r(846, 19)$.
E109 $q(3477, 2190)$.
E110 $r(3477, 2190)$.
E111 $q(6991, 1885)$.
E112 $r(6991, 1885)$.
Compute the following:
E113 $GCD(60, 90)$.
E114 $LCM(60, 90)$.
E115 $GCD(192, 318)$.
E116 $LCM(192, 318)$.
E117 $GCD(1992, 432)$.
E118 $GCD(5005, 11011)$.
E119 $GCD(0, 58)$.
E120 $LCM(99, 0)$.
E121 $GCD(0, 0)$.
E122 $GCD(192, 318)$.
E123 $GCD(2118, 713)$.
E124 Are 218 and 5444 coprime?
E125 Are 4730 and 13671 coprime?.
E126 Find $GCD(79507, 5547)$ without using Euclid's algorithm. You may use the fact that $79507 = 43^3$ and $5547 = 3 \cdot 43^2$.
Find the prime factorization of the following six integers:
E127 343
E128 3280
E129 4114
E130 10989
E131 2592
E132 17303
E133 Compute $GCD(10989, 17303)$.

2.2.8 Problems

P7 Prove that "a divides b" is a reflexive and transitive relation on $\mathbb{Z}$.

Try to determine whether the following two statements are true or false. You may begin by checking whether the statement holds or not for some small values of n.

P8 For all $n \in \mathbb{Z}^+$, the following formula holds:

$$1 + 2 + 3 + \ldots + n = \frac{n(n+1)}{2}$$

P9 Let n be an integer. Then $n^2 + n + 17$ is always a prime number.

2.3 Ideals

We shall now discuss certain subsets of $\mathbb{Z}$ which are very important.

Definition 12. An *ideal* is a subset of $\mathbb{Z}$ of the following form:

$$\{x \in \mathbb{Z} \mid x \text{ is a multiple of } m\}$$

for some integer m. We write $\langle m \rangle$ for this ideal.

Example 26. The ideal $\langle 5 \rangle$ is the set

$$\{\ldots, -10, -5, 0, 5, 10, 15, 20, \ldots\}$$

Example 27. The ideal $\langle 12 \rangle$ is the set

$$\{\ldots, -24, -12, 0, 12, 24, 36, 48, \ldots\}$$

Example 28. The ideal $\langle 0 \rangle$ is the set $\{0\}$. This ideal is called the *zero ideal*.

Note that every ideal except the zero ideal is an infinite set, containing both negative and positive numbers, and also the number zero.

Definition 13. For a nonzero ideal, we define the *generator* of the ideal to be the smallest positive element of the ideal. The generator of the zero ideal is defined to be the number 0.

Example 29. The generator of the ideal

$$\{\ldots, -6, -3, 0, 3, 6, 9, 12, 15, \ldots\}$$

is the number 3.

Note that the generator is defined so that any ideal is the set of all multiples of its generator.

Theorem 5. A nonempty subset M of $\mathbb{Z}$ is an ideal if and only if it is closed under subtraction. (This last condition means that whenever n and k are in M, then $(n-k)$ is also in M.)

Proof. Omitted. □

Definition 14. Let $a, b \in \mathbb{Z}$. A *linear combination* of a and b is an integer of the form $xa + yb$ for some $x, y \in \mathbb{Z}$. The set of all linear combinations of a and b is denoted by $\langle a, b \rangle$.

Example 30. Some examples of linear combinations of a and b:

$$2a + 3b\ , \quad 10a - b\ , \quad b\ , \quad -a - 100b$$

Example 31. 8 is a linear combination of 12 and 26, because we have $8 = 5 \cdot 12 - 2 \cdot 26$. Another example: 1 is a linear combination of 10 and 7, because we have $1 = 5 \cdot 10 - 7 \cdot 7$.

The set $\langle a, b \rangle$ is the set of all integers that can be reached from 0, using only jumps of length a and b. For example, the last example shows that making five jumps of length 12 in the positive direction and then two jumps of length 26 in the negative direction takes us to the number 8. Similarly, we can reach 1 by jumping five jumps of length 10 in the positive direction, and then seven jumps of length 7 in the negative direction.

Theorem 6. Let a and b be two integers. Then the set $\langle a, b \rangle$ is an ideal.

Proof. It is enough to show that the set is closed under subtraction. So let n and k be two elements of $\langle a, b \rangle$. Then we have

$$n = x_1 a + y_1 b$$
$$k = x_2 a + y_2 b$$

for some integers x_1, x_2, y_1, y_2. But we see that

$$n - k = (x_1 - x_2) \cdot a + (y_1 - y_2) \cdot b$$

which shows that $(n-k)$ is also a linear combination of a and b. Hence we can conclude that $\langle a, b \rangle$ is closed under subtraction. □

Theorem 7. The generator of $\langle a, b \rangle$ is equal to $GCD(a, b)$.

Proof. We consider two different cases, and use a separate argument for each case. In the proof of Case 2, we use the following three facts:

- If $d|a$ and $d|b$, then d divides every linear combination of a and b.
- If $d|a$ and $d|b$, then d also divides $GCD(a, b)$.

- If two positive integers divide each other, then they must be equal.

Case 1: $\langle a, b\rangle$ is the zero ideal. This means that every linear combination of a and b is equal to 0. Since a is a linear combination of a and b, we see that $a = 0$. For the same reason, $b = 0$. So from the definition of GCD, we see that $GCD(a, b) = 0$. Clearly this is equal to the generator of $\langle a, b\rangle$.
Case 2: $\langle a, b\rangle$ is not the zero ideal. Let d be the generator of $\langle a, b\rangle$. It is a positive number. Since it is a linear combination of a and b, there are integers x, y such that $d = xa + by$. By definition of GCD, the number $GCD(a, b)$ divides a, and it also divides b. Hence it must divide d (by the first fact above).
The set $\langle a, b\rangle$ is the set of all multiples of the generator d. Since a and b are elements of $\langle a, b\rangle$, both a and b are multiples of d. Therefore, (by the second fact above), d must divide $GCD(a, b)$. Now d and $GCD(a, b)$ are positive integers dividing each other, so they must be equal (third fact above). □

Theorem 8 (Bezout's theorem)**.** Let $a, b \in \mathbb{Z}$. Then $GCD(a, b)$ can be written as a linear combination of a and b.

Proof. The previous theorem shows that $GCD(a, b)$ is an element of $\langle a, b\rangle$. □

Theorem 9. The intersection of two ideals is an ideal.

(I forgot to prove this in class, but include it here for completeness.)

Proof. Let I and J be two ideals. Then they are both closed under subtraction, and they both contain the number 0. Let n and k are any elements of the intersection $I \cap J$. Then because n and k are in I, the difference $(n - k)$ is also an element of I. For the same reason we see that $(n - k)$ is in J. But this implies that $(n - k)$ is an element of $I \cap J$. Hence $I \cap J$ is closed under subtraction , so it is an ideal. (It is nonempty because it contains the number 0.) □

Theorem 10. The generator of $\langle a\rangle \cap \langle b\rangle$ is equal to $LCM(a, b)$.

Proof. Again we consider two different cases.
Case 1: At least one of a and b equals zero.
In this case one of the sets $\langle a\rangle$ and $\langle b\rangle$ (or both) is the zero ideal. Hence the intersection $\langle a\rangle \cap \langle b\rangle$ is the zero ideal, and its generator is 0. We also have $LCM(a, b) = 0$, by definition of LCM.
Case 1: a and b are both nonzero.
We know that

- $\langle a\rangle$ is the set of all multiples of a
- $\langle b\rangle$ is the set of all multiples of b

Hence the intersection of the two ideals is the set of integers that are a multiple of a *and* a multiple of b. Since $LCM(a,b)$ has this property, it is an element of $\langle a\rangle \cap \langle b\rangle$. We must show that $LCM(a,b)$ is actually the *smallest* positive element of $\langle a\rangle \cap \langle b\rangle$. But this follows immediately from the definition of LCM. □

Theorem 11 ("To divide is to contain")**.** Let a and b be integers. Then $a|b$ if and only if $\langle a\rangle \supseteq \langle b\rangle$.

Proof. There are two things to prove.
Part 1: $a|b \implies \langle a\rangle \supseteq \langle b\rangle$.
Suppose that a divides b. Then $b = ac$ for some c. Hence every multiple of b is also a multiple of a. Hence the set of all multiples of b is a subset of the set of all multiples of a, so $\langle a\rangle \supseteq \langle b\rangle$.
Part 2: $\langle a\rangle \supseteq \langle b\rangle \implies a|b$.
Suppose that $\langle a\rangle \supseteq \langle b\rangle$. Since b is an element of $\langle b\rangle$, it must then also be an element of $\langle a\rangle$. This means that b is a multiple of a, that is $a|b$. □

2.3.1 Exercises

Are the following three sets examples of ideals?
E134 The set of positive integers.
E135 The set of even integers.
E136 The set of prime numbers.
E137 Write down some elements of $\langle 9\rangle$.
E138 Write down some elements of $\langle 7\rangle \cap \langle 3\rangle$.
E139 What is the generator of $\langle 191\rangle$?
E140 What is the generator of $\langle 6\rangle \cap \langle 9\rangle$?
E141 How many elements of the ideal $\langle 7\rangle$ are positive and smaller than 55?
E142 Is 14 a linear combination of 2 and 6 ?
E143 Is 9 a linear combination of 2 and 6 ?
Compute the generators of the following ideals:
E144 $\langle 4, 9\rangle$
E145 $\langle 114, 216\rangle$
E146 $\langle 50700, 8424\rangle$
E147 $\langle 4\rangle \cap \langle 3\rangle$
E148 $\langle 16\rangle \cap \langle 18\rangle$
Use the previous exercises to answer the following questions:
E149 Is 17 a linear combination of 4 and 9?
E150 Is 18911 a linear combination of 4 and 9?
E151 Is 18 a linear combination of 114 and 216?
E152 Is 2 a linear combination of 114 and 216?
E153 Is 258 a linear combination of 114 and 216?
E154 Is 1092 a linear combination of 8424 and 50700?