

PROBLEM SET 3: ELEMENTARY NUMBER THEORY

HARM DERKSEN

1. GCD

If d and n are integers, then we say that d divides n if and only if there exists an integer q such that $n = qd$. Notice that if d divides n and m , then d also divides $n + m$ and $n - m$ and $an + bm$ for all integers a, b .

Theorem 1. *If n and m are integers and $m \neq 0$, then there exists an integer q such that*

$$n = qm + r$$

where $0 \leq r < |m|$.

Proof. First reduce to the case that $n \geq 0$. Then use induction on n . (Exercise.) □

A useful variation is the following result.

Theorem 2. *If n and m are integers and $m \neq 0$, then there exists an integer q such that*

$$n = qm + r$$

where $-|m|/2 \leq r < |m|/2$.

Suppose that n and m are integers, not both equal to 0. The greatest common divisor of n and m is the largest *positive* integer d such that d divides both n and m . We denote the greatest common divisor of n and m by $\gcd(n, m)$. We will also use the convention that $\gcd(0, 0) = 0$. The following observation will be useful.

Lemma 1. *If $n, m, q \in \mathbb{Z}$, then We have $\gcd(n, m) = \gcd(m, n - qm)$.*

Proof. The case $n = m = 0$ is clear. Assume that at least one of n and m is nonzero. Now $\gcd(n, m)$ divides n , m and $n - qm$, hence

$$\gcd(n, m) \leq \gcd(m, n - qm).$$

On the other hand, $\gcd(m, n - qm)$ divides m , $n - qm$ and $n = (n - qm) + qm$. so

$$\gcd(m, n - qm) \leq \gcd(n, m).$$

□

Example 1. Suppose we have two large integers, say 9081 and 3270. How do we find their greatest common divisor? We do division with remainder:

$$(1) \quad 9081 = 3 \cdot 3270 - 729.$$

Now $\gcd(9081, 3270) = \gcd(3270, 729)$. We have simplified our problem! Now we can play this game again:

$$(2) \quad 3270 = 4 \cdot 729 + 354.$$

so $\gcd(3270, 729) = \gcd(729, 354)$.

$$(3) \quad 729 = 2 \cdot 354 + 21$$

so $\gcd(729, 354) = \gcd(354, 21)$.

$$(4) \quad 354 = 17 \cdot 21 - 3$$

so $\gcd(354, 21) = \gcd(21, 3) = 3$ because $21 = 7 \cdot 3$. We have found that $\gcd(9081, 3270) = 3$. This method of computing the gcd is called Euclid's algorithm.

Algorithm 1 (Euclid's Algorithm). Suppose that $r_0, r_1 \in \mathbb{Z}$ are nonzero integers. Define $q_1, q_2, \dots \in \mathbb{Z}$ and $r_2, r_3, \dots \in \mathbb{Z}$ inductively as follows. If r_{i-1} and r_i are already defined, then we define q_i and r_{i+1} by

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

where $0 \leq r_{i+1} < |r_i|$ as in Theorem 1 (or $-|r_i|/2 \leq r_{i+1} < |r_i|/2$ as in Theorem 2). (Note r_{i+1} and q_i are well defined as long as $r_i \neq 0$).

Since $|r_1| > |r_2| > \dots$ we have that $r_{k+1} = 0$ for some positive integer k . Suppose that $r_{k+1} = 0$ and that $r_i \neq 0$ for $i \leq k$. Then $\gcd(r_0, r_1) = r_k$.

If one uses Theorem 2 then it is clear that Euclid's algorithm is very fast. The number of divisions with remainder one has to do is roughly $\log_2 |r_1|$. (A similar bound also holds if one uses Theorem 1 though).

Proof. It is not hard to show that Euclid's algorithm works. Note that $\gcd(r_{i-1}, r_i) = \gcd(r_i, r_{i+1})$ for all i . By induction on i one shows that $\gcd(r_0, r_1) = \gcd(r_i, r_{i+1})$ for all i . In particular,

$$\gcd(r_0, r_1) = \gcd(r_k, r_{k+1}) = \gcd(r_k, 0) = r_k.$$

☺

Example 2. Euclid's algorithm can be used to find integers x and y such that $\gcd(n, m) = xn + ym$. It works as follows. First use Euclid's algorithm to compute $\gcd(n, m)$ and then work back. For example, we already saw that $\gcd(9081, 3270) = 3$. We would like to find x and y such that

$$3 = 9081x + 3270y.$$

Now we work back in the computation of $\gcd(9081, 3270)$. From (4) follows that

$$3 = (-1) \cdot 354 + 17 \cdot 21.$$

From (3) follows that

$$3 = (-1) \cdot 354 + 17 \cdot (729 - 2 \cdot 354) = 17 \cdot 729 + (-1 - 17 \cdot 2) \cdot 354 = 17 \cdot 729 - 35 \cdot 354.$$

From (2) follows that

$$\begin{aligned} 3 &= 17 \cdot 729 - 35 \cdot (3270 - 4 \cdot 729) = \\ &= -35 \cdot 3270 + (17 + 35 \cdot 4) \cdot 729 = -35 \cdot 3270 + 157 \cdot 729. \end{aligned}$$

and finally, from (1) follows that

$$\begin{aligned} 3 &= -35 \cdot 3270 + 157 \cdot (-9081 + 3 \cdot 3270) = \\ &= -157 \cdot 9081 + (-35 + 3 \cdot 157) \cdot 3270 = -157 \cdot 9081 + 436 \cdot 3270. \end{aligned}$$

This method is sometimes called the *extended Euclid's algorithm*.

Algorithm 2. (Extended Euclid's Algorithm) Let $r_0, r_1, \dots, r_k, r_{k+1} = 0$ and q_0, q_1, \dots, q_k as in Algorithm 1.

Define $x_k = 0$ and $x_{k+1} = 1$. For $i \geq 1$, define x_{k-i} by induction by

$$x_{k-i-1} = x_{k-i+1} - q_{k-i}x_{k-i}.$$

Then we have that

$$\gcd(r_0, r_1) = x_{i+1}r_i + x_i r_{i+1}$$

for $i = 0, 1, \dots, k$. In particular,

$$\gcd(r_0, r_1) = x_1 r_0 + x_0 r_1.$$

Proof. Let $i = k - j$. We prove by induction on j that

$$\gcd(r_0, r_1) = x_{k-j+1}r_{k-j} + x_{k-j}r_{k-j+1}.$$

For $j = 0$ we have to prove that

$$\gcd(r_0, r_1) = 1 \cdot r_k + 0 \cdot r_{k+1} = r_k$$

but this follows from Algorithm 1.

Suppose that

$$\gcd(r_0, r_1) = x_{k-j+1}r_{k-j} + x_{k-j}r_{k-j+1}.$$

If we substitute, $r_{k-j+1} = r_{k-j-1} - q_{k-j}r_{k-j}$ we obtain

$$\begin{aligned} \gcd(r_0, r_1) &= x_{k-j+1}r_{k-j} + x_{k-j}(r_{k-j-1} - q_{k-j}r_{k-j}) = \\ &= x_{k-j}r_{k-j-1} + (x_{k-j+1} - q_{k-j}x_{k-j})r_{k-j} = x_{k-j}r_{k-j-1} + x_{k-j-1}r_{k-j}. \end{aligned}$$



Theorem 3. *Suppose that n and m are integers. There exist integers x and y such that*

$$\gcd(n, m) = xn + ym.$$

Proof. This follows from the extended Euclid's Algorithm (Algorithm 2). ☺
If n and m are integers with $\gcd(n, m)$ then we say that m and n are *relatively prime*.

Corollary 1. *If a, n, m are integers and a divides both n and m then a also divides $\gcd(n, m)$.*

Proof. This follows immediately from the previous Theorem 3. □

Example 3 (Putnam 2000). Prove that the expression

$$\frac{\gcd(m, n)}{n} \binom{n}{m}$$

is an integer.

Discussion. Given our previous discussion, it seems natural to write

$$\gcd(m, n) = xm + yn$$

where x, y are integers. The solution then follows quickly.

Proof. We can write

$$\gcd(m, n) = xm + yn$$

where $x, y \in \mathbb{Z}$. Then

$$\frac{\gcd(m, n)}{n} \binom{n}{m} = x \binom{n}{m} + y \frac{m}{n} \binom{n}{m}.$$

Now

$$\frac{m}{n} \binom{n}{m} = \frac{m}{n} \frac{n!}{m!(n-m)!} = \frac{(n-1)!}{(m-1)!(n-m)!} = \binom{n-1}{m-1}$$

is an integer. It follows that

$$\frac{\gcd(m, n)}{n} \binom{n}{m}$$

is an integer. ☺

Lemma 2. *Suppose that n, m, r are integers such that $\gcd(m, n) = 1$. If m divides nr then n divides r .*

Proof. We can write $1 = xm + yn$ for certain $x, y \in \mathbb{Z}$. Clearly m divides xmr and ynr , so m divides

$$r = r \cdot 1 = r \cdot (xm + yn) = xmr + ynr.$$

□

If n and m are nonzero integers then the least common multiple $\text{lcm}(m, n)$ of n and m is defined as the smallest positive integer that is divisible by both m and n . Moreover we define $\text{lcm}(m, 0) = 0$ for all integers m .

Lemma 3. *If n and m are positive integers and a is an integer divisible by both n and m , then a is divisible by $\text{lcm}(m, n)$.*

Proof. We can write $a = q\text{lcm}(m, n) + r$ with $0 \leq r < \text{lcm}(m, n)$. Now r is also divisible by m and n . We must have that $r = 0$ otherwise we get a contradiction with the definition of $\text{lcm}(m, n)$. This proves that a is divisible by $\text{lcm}(m, n)$. \square

Lemma 4. *If n and m are positive integers then*

$$\text{gcd}(m, n) \text{lcm}(m, n) = mn$$

Proof. The positive integer $mn/\text{gcd}(m, n)$ is divisible by m and n , so

$$\frac{mn}{\text{gcd}(m, n)} \geq \text{lcm}(m, n).$$

The positive integer $mn/\text{lcm}(m, n)$ divides both m and n . So we have

$$\frac{mn}{\text{lcm}(m, n)} \leq \text{gcd}(m, n).$$

\square

Example 4. In the strange country Oz, the only official coins are the 7-cents coin and the 13-cents coin. What is the largest amount that cannot be paid with these coins if a shop has no change at all?

Discussion. We can first make a list of amounts that we can make:

7, 13, 14, 20, 21, 26, 27, 28, 33, 34, 35, 39, 40, 41, 42, 46, 48, 48, 49, 52, 53, 54, 55, 56,

59, 60, 61, 62, 63, 65, 66, 67, 68, 69, 70, 72, 73, 74, 75, 76, 77, 78, 79, ...

The largest amount that cannot be made seems to be 71. It is easy to check that 71 is not a nonnegative combination of 7 and 13.

Let us try to understand why all the amounts of ≥ 72 can be made by using the two types of coins. Suppose that $m \geq 72$. We would like to find nonnegative integers x and y such that

$$m = 13x + 7y$$

If x and y are not necessarily nonnegative then this is certainly possible. We can write

$$1 = 13 \cdot (-1) + 7 \cdot 2$$

and

$$m = 13 \cdot (-m) + 7 \cdot 2m.$$

Using this solution we find many other solutions. If k is an integer then

$$m = 13 \cdot (-m + 7k) + 7 \cdot (2m - 13k).$$

For a suitable k , we might have that both $-m + 7k$ and $2m - 13k$ are nonnegative. Consider the smallest k for which $-m + 7k$ is nonnegative. Then we have $0 \leq -m + 7k < 7$. Now

$$7 \cdot (2m - 13k) \geq m - 13 \cdot (-m + 7k) \geq 72 - 13 \cdot 6 = -6.$$

It follows that $2m - 13k > -1$, so $2m - 13k$ is nonnegative.

Now we would like to prove that if

$$(5) \quad 71 = 13x + 7y$$

with $x, y \in \mathbb{Z}$, then at least one of the integers x, y is negative. We already saw one solution, namely

$$(6) \quad 71 = 13 \cdot (-71) + 7 \cdot (142).$$

Combining (5) and (6) yields:

$$13 \cdot (x + 71) = 7 \cdot (142 - y).$$

Since $\gcd(13, 7) = 1$, we have that 7 divides $x + 71$. Say $x + 71 = 7k$. Then we also have that $142 - y = 13k$. From $x + 71 = 7k$ and $x \geq 0$ follows that $k \geq 11$. But then $y = 142 - 13k \leq -1$.

Problem 1. ** Let F_0, F_1, F_2, \dots be the Fibonacci numbers: $F_0 = F_1 = 1$ and $F_{n+1} = F_n + F_{n-1}$ for all $n \geq 1$. Prove that the greatest common divisor of two consecutive Fibonacci numbers is always equal to 1.

Problem 2. *** Define T_0, T_1, T_2, \dots by $T_1 = 2$ and $T_{n+1} = T_n^2 - T_n + 1$ for $n \geq 0$. Prove that $\gcd(T_i, T_j) = 1$ for all $i \neq j$.

Problem 3. **** Let $m \geq 2$ be an integer and suppose that a and b are positive integers. Prove that

$$\gcd(m^a - 1, m^b - 1) = m^{\gcd(a, b)} - 1.$$

Problem 4. ** We have two drinking glasses. One glass can contain exactly 21oz. The other glass can contain exactly 13oz. Is it possible to measure exactly 1oz. of water using the two glasses?

2. PRIME NUMBERS

Recall that a prime number is a positive integer with exactly 2 positive divisors, namely 1 and itself.

Lemma 5. *If p is a prime number dividing mn where m and n are integers, then p divides m or p divides n .*

Proof. If p divides m then we are done. Otherwise $\gcd(p, m) = 1$, so p divides n by Lemma 2. \square

Theorem 4. (Euclid) *Every positive integer can uniquely be written as a product of prime numbers.*

Proof. We already have seen in problem set 1 that every positive integer is a product of prime numbers. We still have to prove the uniqueness. Suppose that $p_1 < p_2 < \cdots < p_k$ are distinct prime numbers such that

$$p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} = p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}.$$

Suppose that $a_1 > b_1$. Then

$$p_1^{a_1-b_1} p_2^{a_2} \cdots p_k^{a_k} = p_2^{b_2} \cdots p_k^{b_k}$$

and p_1 divides $p_2^{b_2} \cdots p_k^{b_k}$. This implies that p_1 divides p_i for some $i \geq 2$. This is impossible because the only divisors of p_i are 1 and p_i itself. Contradiction. Therefore $a_1 \leq b_1$. Similarly we see that $a_1 \geq b_1$ and therefore $a_1 = b_1$. Similarly we can prove that $a_i = b_i$ for $i = 2, 3, \dots, k$. \square

Many properties can be expressed in terms of the prime factorization. Suppose that

$$A = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$$

and

$$B = p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}$$

are positive integers with their factorizations into prime numbers. Then A divides B if and only if $a_i \leq b_i$ for all $i = 1, 2, \dots, k$. We also have that

$$\gcd(A, B) = p_1^{c_1} p_2^{c_2} \cdots p_k^{c_k}$$

where $c_i = \min(a_i, b_i)$ for all i .

Theorem 5. (Euclid) *There are infinitely many prime numbers.*

Proof. Suppose that there are finitely many distinct prime numbers, say p_1, p_2, \dots, p_k . Let $N = p_1 p_2 \cdots p_k + 1$. Now N is a product of prime numbers. In particular there exists a prime number q such that q divides N . Now $q = p_i$ for some i with $1 \leq i \leq k$. Since p_i divides N , we have that p_i divides

$$N - p_1 p_2 \cdots p_k = 1$$

which leads to a contradiction. \square

Example 5. The number $\sqrt{2}$ is irrational.

Proof. Suppose that $\sqrt{2}$ is rational, say $\sqrt{2} = p/q$ where p, q are positive integers. Squaring gives $p^2 = 2q^2$. The prime number 2 appears an even number of times in the prime factorization of p^2 . On the other hand, 2 appears an odd number of times in the prime factorization of $2q^2$. We get a contradiction, so $\sqrt{2}$ has to be irrational. \square

The distribution of prime numbers is quite mysterious. One of the most famous/notorious open problems in mathematics is the Riemann Hypothesis. This conjecture is closely related to the distribution of prime numbers. The following result is well-known but not so elementary:

Theorem 6 (Dirichlet). *Suppose that a and b are positive integers that are relatively prime. Then there are infinitely prime numbers of the form $a + nb$ where n is a positive integer.*

Problem 5. ** Suppose that

$$A = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$$

is an integer, $p_1 < p_2 < \cdots < p_k$ are distinct primes and a_1, \dots, a_k are nonnegative integers. Give a formula for the number of divisors of A .

Problem 6. *** Suppose that

$$A = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$$

is an integer, $p_1 < p_2 < \cdots < p_k$ are distinct primes and a_1, \dots, a_k are nonnegative integers. Give a formula for the *sum* of divisors of A .

Problem 7. *** We start with a deck of 52 cards. We put all the cards in one row, face down. In the first round we turn all the cards around. In the second round we turn every second card around. In the third round we turn every third card around. We keep doing this until we complete round 52. Which cards will be faced up in the end?

Problem 8. *** Suppose that $P(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$ is a nonconstant polynomial with integer coefficients. Prove that there exists a positive integer m such that $|P(m)|$ is not a prime number.

Problem 9. ** Show that there are infinitely many prime numbers of the form $4k - 1$ where k is a positive integer (without using Dirichlet's Theorem).

Problem 10. * Find all prime numbers p for which $p + 2$ and $p + 4$ are also prime numbers.

3. THE CHINESE REMAINDER THEOREM

Suppose that m is an integer. We say that a is congruent to b modulo m if m divides the difference $a - b$. The notation we use is

$$a \equiv b \pmod{m}.$$

Notice that if $a_1 \equiv b_1 \pmod{m}$ and $a_2 \equiv b_2 \pmod{m}$ then

$$a_1 + a_2 \equiv b_1 + b_2 \pmod{m}$$

and

$$a_1 a_2 \equiv b_1 b_2 \pmod{m}.$$

Theorem 7. *Suppose that m and n are positive integers such that $\gcd(m, n) = 1$. Suppose that a and b are integers. Then there is a unique integer c with $0 \leq c < mn$ such that*

$$c \equiv a \pmod{m}$$

and

$$c \equiv b \pmod{n}$$

Proof. We find can find integers $x, y \in \mathbb{Z}$ such that $xm + yn = 1$. Note that $xm \equiv 1 \pmod{n}$ and $yn \equiv 1 \pmod{m}$. Consider $d = bxm + ayn$. We can write $d = qmn + c$ with $0 \leq c < mn$. Then

$$c \equiv d \equiv ayn \equiv a \pmod{m}$$

and

$$c \equiv d \equiv bxm \equiv b \pmod{n}.$$

This shows the existence of c . Suppose that c' is another integer with $c' \equiv a \pmod{m}$, $c' \equiv b \pmod{n}$ and $0 \leq c' < mn$. Then $c - c'$ is divisible by m and by n . Because $\gcd(m, n) = 1$, $c - c'$ is divisible by mn . Since $|c - c'| < mn$ we must have that $c = c'$. \square

The previous theorem easily can be generalized as follows.

Theorem 8. Suppose that m_1, m_2, \dots, m_k are pairwise relatively prime positive integers (so $\gcd(m_i, m_j) = 1$ for $i \neq j$). Suppose that a_1, a_2, \dots, a_k are integers. Then there is a unique integer c with $0 \leq c < m_1 m_2 \cdots m_k$ such that

$$c \equiv a_i \pmod{m_i}$$

for $i = 1, 2, \dots, k$.

Example 6. Show that the difference of two consecutive prime numbers can be arbitrarily large.

Discussion. We want to show that for every m there exists an n such that $n + 1, n + 2, \dots, n + m$ are not prime. Let us assume that $n + 1$ is divisible by 2 and that $n > 2$. Then $n + 1$ is not a prime number. Now $n + 2$ is not divisible by 2. However, we could assume that $n + 2$ is divisible by 3 and $n + 2 > 3$. Then $n + 2$ is certainly not a prime either. Similarly we could assume that $n + 3$ is divisible by 5 and $n + 3 > 5$. The Chinese Remainder Theorem comes to the rescue.

Proof. Let p_1, p_2, \dots, p_m be the first m prime numbers. Using the Chinese Remainder theorem we can find an integer c such that

$$n \equiv -i \pmod{p_i}$$

for $i = 1, 2, \dots, m$. Without loss of generality we may assume that $n > p_i$ for all i (otherwise we may add a multiple of $p_1 p_2 \cdots p_m$ to n). For every i in $\{1, 2, \dots, m\}$ we see that p_i divides $n + i$ but $c + i > p_i$. This shows that $c + i$ is not a prime number. ☺

A slightly easier proof is the following.

Proof. For every n , consider the numbers

$$n! + 2, n! + 3, \dots, n! + n.$$

all these numbers are not prime numbers because $n! + i$ is divisible by i . ☺

Problem 11. ***[Gardner, M., *The Monkey and the Coconuts*, Ch. 9 in *The Second Scientific American Book of Puzzles & Diversions: A New Selection*. New York: Simon and Schuster, pp. 104-111, 1961.] Five sailors survive a shipwreck and swim to a tiny island where there is nothing but a coconut tree and a monkey. The sailors gather all the coconuts and put them in a big pile under the tree. Exhausted, they agree to go to wait until the next morning to divide up the coconuts.

At one o'clock in the morning, the first sailor wakes. He realizes that he can't trust the others, and decides to take his share now. He divides the coconuts into five equal piles, but there is one left over. He gives that coconut to the monkey, buries his coconuts, and puts the rest of the coconuts back under the tree.

At two o'clock, the second sailor wakes up. Not realizing that the first sailor has already taken his share, he too divides the coconuts up into five piles, leaving one over which he gives to the monkey. He then hides his share, and piles the remainder back under the tree.

At three, four and five o'clock in the morning, the third, fourth and fifth sailors each wake up and carry out the same actions.

In the morning, all the sailors wake up, and try to look innocent. No one makes a remark about the diminished pile of coconuts, and no one decides to be honest and admit that they've already taken their share. Instead, they divide the pile up into five piles, for the sixth time, and find that there is yet again one coconut left over, which they give to the monkey.

How many coconuts were there originally? (Find the smallest number of coconuts that is consistent with this story.)

4. EULER'S FUNCTION

For an integer n we define $\phi(n)$ as the number of elements in the set

$$\{a \in \mathbb{Z} \mid 1 \leq a \leq n, \gcd(a, n) = 1\}$$

of all positive integers a which are relatively prime to n .

Lemma 6. *If m and n are positive integers then $\phi(mn) = \phi(m)\phi(n)$.*

Proof. Given $c \in \{1, 2, \dots, mn\}$ we can find unique $a \in \{1, 2, \dots, n\}$ and $b \in \{1, 2, \dots, m\}$ such that

$$(7) \quad c \equiv a \pmod{n}$$

and

$$(8) \quad c \equiv b \pmod{m}.$$

Conversely, given $a \in \{1, 2, \dots, n\}$ and $b \in \{1, 2, \dots, m\}$ there exists a unique $c \in \{1, 2, \dots, mn\}$ such that (7) and (8) hold by the Chinese remainder theorem. We have

$$\gcd(c, mn) = \gcd(c, m) \gcd(c, n) = \gcd(a, n) \gcd(b, m).$$

So $\gcd(c, mn) = 1$ if and only if $\gcd(a, n) = \gcd(b, m) = 1$. There are $\phi(n)$ choices for a such that $\gcd(a, n) = 1$. There are $\phi(m)$ choices for b such that $\gcd(b, m) = 1$. Therefore, there are $\phi(n)\phi(m)$ choices for a and b such that $\gcd(a, n) = \gcd(b, m) = 1$. So there are $\phi(m)\phi(n)$ choices for c such that $\gcd(c, nm) = 1$. This shows that $\phi(mn) = \phi(m)\phi(n)$. \square

Lemma 7. *If p is a prime number and k is a positive integer then*

$$\phi(p^k) = (p - 1)p^{k-1}.$$

Proof. The elements of

$$\{1, 2, 3, \dots, p^k\}$$

that are not relatively prime to p^k are exactly the p^{k-1} multiples of p . This shows that

$$\phi(p^k) = p^k - p^{k-1} = (p - 1)p^{k-1}.$$

\square

In general if $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ is the prime factorization of n , where $p_1 < p_2 < \cdots < p_k$ are distinct prime numbers and a_1, a_2, \dots, a_k are positive integers, then

$$\phi(n) = (p_1 - 1)p_1^{a_1-1} (p_2 - 1)p_2^{a_2-1} \cdots (p_k - 1)p_k^{a_k-1}.$$

Problem 12. **** Find all integers n for which $\phi(n)$ divides n .

5. EXTRA PROBLEMS

Problem 13. * Use Euclid's Algorithm to find $\gcd(1029, 791)$.

Problem 14. * Use the Extended Euclid's Algorithm to find integers $x, y \in \mathbb{Z}$ such that $268x + 421y = 1$.

Problem 15. ** Find a multiple of 2003 that ends with the digits 9999.

Problem 16. ** Find an integer x such that $x^2 + 1$ is divisible by 130.