UMASS AMHERST MATH 300 SP '05, F. HAJIR

HOMEWORK 8: NUMBER THEORY

1. A little number theory

The set $\mathbb{Z}$ is really much more marvelous than you think. We have already discussed its first marvelous quality: its infinitude. What makes it even more marvelous are the two binary operations $+$ and $\times$. What is a binary operation, you ask? Good question.

Definition 1.1. Let X be a set. A binary operation on a set is a map $\mu : X \times X \to X$. Thus, an operation is a rule, which, given an ordered pair (x, x') of elements of x, produces an element $x'' = \mu(x, x')$ of X in a well-determined way. An alternative notation is often more convenient, namely if $\bullet$ stands for some kind of "operational" symbol, then instead of writing $\mu(x, x')$, we write more compactly $x \bullet x'$. An operation $\bullet$ on X is called *commutative* if $a \bullet b = b \bullet a$ for all $a, b \in X$. It is called *associative* if for all $a, b, c \in X$, $(a \bullet b) \bullet c = a \bullet (b \bullet c)$.

Non-Example 1.2. If $\mathbb{N}$ is the set of natural numbers, ordinary addition $(+)$ defines a commutative operation on $\mathbb{N}$. However, subtraction $(-)$ does not define an operation on $\mathbb{N}$ because for $a, b \in \mathbb{N}$, it is not always the case that $a - b \in \mathbb{N}$.

Example 1.3. The operations $+, \times, -$ on $\mathbb{Z}$ are familiar to you; addition and multiplication are associative and commutative, but subtraction is neither. Why did I leave out $\div$? Well, $\div$ does not actually define an operation on $\mathbb{Z}$ because given $a, b \in \mathbb{Z}$, it is not always that case that $a \div b$ is in $\mathbb{Z}$. Let us define an operation on $\mathbb{Z}$ as follows: given $a, b \in \mathbb{Z}$, we put $a \bullet b = |a^2 - b^2|$. Then $\bullet$ is a well-defined operation on $\mathbb{Z}$. It is clearly commutative. Is it associative?

Going back to what I started with, the set $\mathbb{Z}$ is really marvelous because it has two *compatible* operations $+, \times$ defined on it. What this means is that the two operations "respect" each other: namely, if $a, b, c \in \mathbb{Z}$, then $a \times (b + c) = (a \times b) + (a \times c)$. We say that $\times$ distributes over $+$. Moreover, these operations satisfy a whole host of other properties.[1]

Of the two basic operations $(+, \times)$ on $\mathbb{Z}$, the more subtle of the two is multiplication. How numbers are put together additively is not too mysterious: each integer n decomposes additively into a sum of n 1's: $n = 1 + 1 + \cdots + 1$. As we traverse the number line, this decomposition grows in a regular fashion, picking up one more "1" as it goes. But how numbers decompose *multiplicatively* is much less predictable as we traverse the number line.[2]This comment hopefully serves to explain a little the claim that multiplication is more subtle than addition.

The most subtle and interesting concept then, for the algebraic structure of $\mathbb{Z}$, is that of *divisibility.* Divisibility is a relation on $\mathbb{Z}$ which is transitive and reflexive but not symmetric;

[1] As your study of algebra continues these properties will collectively come to be known as "ring properties"; by the way, "algebra" is the study of sets equipped with certain kinds of operations.

[2] For instance, 17 is indecomposable, $18 = 2 \cdot 3 \cdot 3$, 19 is indecomposable,$20 = 2 \cdot 2 \cdot 5$, $21 = 3 \cdot 7$ etc.

thus it is not an equivalence relation. Its importance is reflected in the multiplicity (excuse the pun) of names for this concept.

Definition 1.4. If n and d are integers, we write $d|n$ if and only if the equation $dx = n$ has a unique solution $x \in \mathbb{Z}$. The following phrases are all equivalent:

- $d|n$,
- d divides n,
- n is a multiple of d,
- n is is divisible by d,
- d is a factor of n,
- d is a divisor of n,
- there exists a unique $x \in \mathbb{Z}$ such that $n = dx$ (in shorthand, we write this as $n/d \in \mathbb{Z}$).

Example 1.5. For any integer $d \in \mathbb{Z}\setminus\{0\}$, we have $d|0$, as the equation $dx = 0$ has a unique solution $x = 0$. On the other hand, the statement $0|n$ is false for every $n \in \mathbb{Z}$, because the equation $0x = n$ has no solutions if $n \neq 0$ and infinitely many solutions if $n = 0$! In summary, 0 **doesn't divide anybody but** 0 **is divisible by everybody other than itself.**

Definition 1.6. For any integer $n \neq 0$, let $\mathrm{Div}(n) = \{d \in \mathbb{Z} \mid d|n\}$ be the set of divisors of n. We let $\mathrm{Div}^+(n) = \{d \in \mathbb{Z} \mid d > 0, d|n\}$ be the set of positive divisors of n and put $\sigma_0(n) = |\mathrm{Div}^+(n)|$.

Since $d \in \mathrm{Div}(n) \Rightarrow |d| \leq |n|$, $\mathrm{Div}(n)$ is a finite set, and in fact, we have the very crude bounds $|\mathrm{Div}(n)| \leq 2n$ and $|\mathrm{Div}^+(n)| \leq n$.

The set $\mathbb{Z} \setminus \{0\}$ is equipped with the involution "multiplication by -1". This involution reduces many issues having to do with multiplicative properties of integers to essentially the same question on the set $\mathbb{N}$ of positive integers. In other words, for every positive divisor of n there is exacly one negative divisor of n, so it suffices to work with $\mathrm{Div}^+(n)$ and this is often more convenient.

Now, suppose $n \in \mathbb{N}$. Every $d \in \mathrm{Div}^+(n)$, can be graphically represented by a $d \times e$ grid of $n = de$ dots arranged in d rows and e columns. We note that $|\mathrm{Div}^+(n)|$ is never empty since $1|n$ and $n|n$, corresponding to the $1 \times n$ and $n \times 1$ arrangements of n points. Now, for certain integers $n \geq 2$, no other rectangular arrangement is possible; these n are called *primes.*

Definition 1.7. A positive integer n is *prime* if $|\mathrm{Div}^+(n)| = 2$. In other words, n is prime if and only if it has exactly two positive divisors, namely 1 and n. An integer n is called *composite* if $|\mathrm{Div}^+(n)| \geq 3$. Thus, every integer > 1 is either prime or composite.

Non-Example 1.8. Note that 1 has but a single positive divisor hence 1 **is not a prime** according to our definition. It is not a composite either! It is clear that it plays a very special role in multiplication, since 1 divides every integer. A number which divides every element of $\mathbb{Z}$ is called *unit.* The only units in $\mathbb{Z}$ are ± 1. The number 1 is further distinguished by its role as the *identity* for multiplication, namely $1 \cdot a = a$ for all $a \in \mathbb{Z}$.

Example 1.9. The primes less than 50 are $2, 3, 5, 7,\ 11, 13, 17, 19, 23, 29,$ 31,37, 41, 43, 47.

The importance of primes for arithmetic is that every integer can be decomposed into a product of primes, and that, up to reordering of the factors, this "prime decomposition" is unique (this is a very important fact, known as The Fundamental Theorem of Arithmetic). Here is an analogy. In this sense, the primes are to arithmetic what "the elements" are to chemistry: we understand molecules in terms of the elements which constitute them. For now, let us show that every integer is a product of primes.

Theorem 1.10. *If $n > 1$ is an integer, then n is a product of primes.*

Proof. We will give a proof by complete mathematical induction. So, for $n \geq 2$, we define the statement $P(n)$ as follows.

$$P(n) : n \text{ is a "product of primes"},$$

which is shorthand for the following more precise statement: there exist primes $p_1, \cdots, p_r$ and positive integerrs $a_1, \ldots, a_r$ such that $n = p_1^{a_1} \ldots p_r^{a_r}$. Note that n is a "product of primes" thus encompasses the possibility that n is a prime itself. Let us check the validity of the base case, i.e. $P(2)$; 2 is a prime, so 2 is a product of primes. We will now proceed to the "induction step" of complete induction, so we have to establish

(*) Given an arbitrary $k \geq 2$, if $P(j)$ holds for $2 \leq j \leq k$, then $P(k+1)$ holds.

The statement (*) can be restated as $P(2) \wedge P(3) \wedge \cdots \wedge P(k) \Rightarrow P(k+1)$. So, we assume for $2 \leq m \leq k$, m is a product of primes and seek to show that $k+1$ is a product of primes. If $k+1$ is a prime itself, then it is a product of primes and we would be done. The other possibility is that $k+1$ is not a product of primes, i.e. $k+1$ is composite (since $k+1 > 1$). Thus, there exist integers $1 < d \leq e < k+1$ such that $de = k+1$. But by the induction hypothesis, since d, e are integers in the range $[2, k]$, each of them is a product of primes, hence so is $k+1 = de$. This establish (*).

We have thus established $P(n)$ for all $n \geq 2$ by complete induction on n. □

Second Proof of Theorem 1.10. Let us now give a proof by contradiction which relies on the Well-ordering principle. The strategy is to use the following lemma.

Lemma 1.11. *If an integer $m \geq 2$ is not a product of primes, then there exists an integer $1 < k < m$ such that k is not a product of primes.*

Proof. Since n is not a product of primes, n itself is not a prime. Since $n \geq 2$, $|\mathrm{Div}^+(n)| \geq 2$, and since n is not prime $|\mathrm{Div}^+(n)| \neq 2$, hence $|\mathrm{Div}^+(n)| > 2$. Therefore, there exists $d \in \mathrm{Div}^+(n) \setminus$ with $1 < d < n$, which implies that $n = de$ with $1 < e < n$ also. Since n is not a product of primes, at least one of d, e must not be a product of primes; since both d and e are in the range $[2, n-1]$, this proves the existence of an integer k, $1 < k < n$ such that k is not a product of primes. □

It should be clear how to prove the theorem using the Lemma. Suppose the theorem is false. Thus, there exists an integer $n \geq 2$ such that n is not a product of primes. Applying the lemma to this n, we get an integer $1 < k_1 < n$. Applying the lemma to k_1, now we get an integer $1 < k_2 < k_1 < n$. It is clear that if we repeat this procedure, we obtain infinitely many integers in the range $[2, n-1]$ which is a contradiction. To be even more precise, repeating this procedure $n-1$ times, we obtain $1 < k_{n-1} < k_{n-2} < \cdots < k_2 < k_1 < n$, i.e. we have $n-1$ distinct integers in the range $[2, n-1]$ which is impossible. This contradiction proves that every integer is a product of primes.

We can rephrase the endgame of this proof a little more efficiently by using the well-ordering principle. If we assume the theorem is false, i.e. that the set

$$\{n \geq 2 \mid n \text{ is not a product of primes}\}$$

is non-empty, then by the well-ordering principle, there exists a least element $m \geq 2$ which is not the product of primes. By the Lemma, there exists $1 < k < m$ such that k is not a product of primes, contradicting the minimality of m. □

The following theorem and proof, going back at least to Euclid, is a classic.

Theorem 1.12. *There are infinitely many primes.*

Proof. How do we show that a set X is infinite? One way to do so would be to show that if $F \subseteq X$ is any non-empty **finite** subset of X, then $X \setminus F$ is non-empty. So, let $\mathbf{P}$ be the set of all primes, and let F be a finite set of primes. Since F is finite, it has a maximal element, say ℓ. Now, define $N = 1 + \prod_{p \leq \ell} p$, i.e. N is one more than the product of all the primes up to and including ℓ. Since $N > 1$, it is a product of primes by the previous theorem, so there exists at least one prime q which divides N. We claim that $q \notin F$. This is because $q|N$ so N/q is an integer, but for $p \in F$, $N/p = x + 1/p$ for some integer x. In other words, for any $p \in F$, when N is divided by p, the remainder is 1, but when N is divided by q, the remainder is 0. Hence, $q \notin F$. We have shown that for every finite subset F of $\mathbf{P}$, $\mathbf{P} \setminus F \neq \emptyset$, hence $\mathbf{P}$ is infinite. □

Recall that for an integer $n \neq 0$, $\operatorname{Div}^+(n)$ is a finite set. If m is another non-zero integer, then $\operatorname{Div}^+(n) \cap \operatorname{Div}^+(m)$ is clearly a finite set and is non-empty since it contains 1, hence it has a unique largest element, which we denote by $\gcd(m, n) = \gcd(n, m)$ and of course call the greatest common divisor of m and n. Apparently the "greatest common factor" is much more à la mode in schools these days. In the reverse direction, for an integer n, we let $n\mathbb{Z} = \{nm \mid m \in \mathbb{Z}\} = \{k \mid k \text{ is divisible by } n\}$ be the set of integer multiples of n. If m and n are non-zero integers, then It is clear that $n\mathbb{Z} \cap m\mathbb{Z} \cap \mathbb{N}$ is not empty since it contains $|mn|$. Thus, this set must have a least element (by the Well-ordering principle) which we call $\operatorname{lcm}(m, n) = \operatorname{lcm}(n, m)$, the least common multiple of m and n.

Calculating the greatest common divisor and least common multiple of pairs of integers is an important computational task in many situtations, so fortunately there is a very efficient procedure for calculating them. It is based on the Division algorithm, which is simply what we usually call Long Division.

Theorem 1.13 (The Division, or Euclidean, Algorithm)**.** *Given integers $n, k \in \mathbb{N}$, there exists a unique pair (q, r) where $q \in \mathbb{N}$ and $r \in \{0, 1, 2, 3, \ldots, k-1\}$ such that $n = qk + r$. We call q the quotient and $r = \operatorname{Rem}[n \div k]$ the remainder of $n \div k$.*

Proof. First let us prove uniqueness of the pair (q, r). Suppose for pairs (q, r) and (q', r') where $q, q' \in \mathbb{N}$ and $r, r' \in \{0, 1, 2, 3, \ldots, k-1\}$, we have $n = qk + r = q'k + r'$. By switching the pairs if necessary, we may assume that $q \geq q'$. Then $(q - q')k = r' - r$. We claim that $q = q'$ and prove this by contradiction. If not, then $q - q' > 0$ and $k \geq 1$ together imply that $r' - r = (q - q')k \geq k$ which in turn implies that $r' \geq k$ since $r \geq 0$, but $r' < k$ by assumption, giving the desired contradiction. Thus, $q = q'$, and since $r' - r = (q - q')k$, we get $r' = r$ also. This proves uniqueness of the specified pair (q, r). Now let us establish the existence of this pair.

Since $k \neq 0$ by assumption, the set $S = \{x \in \mathbb{N} \mid xk \leq n\}$ is finite. It therefore has a largest element; we put $q = \max S$ for this maximal element, and let $r = n - qk$. It remains to show that $0 \leq r \leq k-1$. Since $q \in S$, $qk \leq n$ so $r = n - qk \geq 0$. To show that $r \leq k-1$, let us use proof by contradiction. If $r \geq k$, then

$$n = qk + r = qk + k + r - k = (q+1)k + (r-k),$$

which, since $r - k \geq 0$ would show that $q+1 \in S$ contradicting the fact that $q = \max S$. Thus $0 \leq r \leq k-1$. □

The division algorithm can be used to calculate the greatest common divisor of two given positive integers efficiently. Let us examine the key idea. Given $n_1, n_2 \geq 1$, we rearrange them if necessary to have $n_1 \geq n_2$. If $n_1 = n_2$, then we rejoice because then $\gcd(n_1, n_2) = n_2$ without any further ado. The strategy is to replace the pair (n_1, n_2) by a **smaller** pair (n_2, n_3) with the **same** gcd! So where do we get n_3 from? Easy, we take n_3 to be the remainder when n_1 is divided by n_2! Thus, we need to prove a little lemma.

Lemma 1.14. *If $n \geq k \geq 1$ and $n = qk + r$ with $q \in \mathbb{N}$, then $\gcd(n,k) = \gcd(k,r)$.*

Proof. Recall that $\gcd(n,k)$ is by definition the largest element of $\mathrm{Div}^+(n) \cap \mathrm{Div}^+(k)$, thus it suffices to prove that

$$\mathrm{Div}^+(n) \cap \mathrm{Div}^+(k) = \mathrm{Div}^+(k) \cap \mathrm{Div}^+(r).$$

To prove the above equality of sets, we well show that each set is contained in the other. So, suppose $d|n$ and $d|k$. Then $d|qk$ so $d|(n-qk)$ i.e. $d|r$. So now $d|k$ and $d|r$ showing that $\mathrm{Div}^+(n) \cap \mathrm{Div}^+(k) \subseteq \mathrm{Div}^+(k) \cap \mathrm{Div}^+(r)$. On the other hand, if $d|r$ and $d|k$, then $d|qk$ so $d|(qk+r)$ i.e. $d|n$, showing the reverse inclusion. This completes the proof of the lemma. □

The strategy for computing $\gcd(n_1, n_2)$ should now be clear. Let $n_3 = \mathrm{Rem}[n_1 \div n_2]$, and indeed for each $i \geq 3$, successively define $n_i = \mathrm{Rem}[n_{i-2} \div n_{i-1}]$. Then, $n_2 > n_3 > \cdots$ gives a strictly decreasing sequence of remainders (which are automatically non-negative!), i.e. $n_2 > n_3 > \cdots \geq 0$, thus this sequence must eventually hit 0. Let $s \geq 2$ be the least integer such that $n_s = 0$. Thus, we have

$$\gcd(n_1, n_2) = \gcd(n_2, n_3) = \cdots = \gcd(n_{s-2}, n_{s-1}) = \gcd(n_{s-1}, 0), \qquad n_{s-1} \neq 0.$$

Since $n_{s-1} \neq 0$, $\gcd(n_{s-1}, 0) = n_{s-1}$. Another perspective is that since $n_s = \mathrm{Rem}[n_{s-2} \div n_{s-1}] = 0$, we have $n_{s-1}|n_{s-2}$ and hence $\gcd(n_{s-2}, n_{s-1}) = n_{s-1}$. Either way, we find $\gcd(n_1, n_2) = n_{s-1}$ is the penultimate remainder (just before getting remainder 0).

Example 1.15. Let us use the above algorithm to compute $\gcd(432, 60)$. So, $n_1 = 432$, $n_2 = 60$. We get $432 = 7 \cdot 60 + 12$ so $n_3 = 12$, and $60 = 5 \cdot 12$ so $n_4 = 0$. Thus, $\gcd(432, 60) = n_3 = 12$. Let's do one more. What is $\gcd(89, 55)$? Letting $n_1 = 89$, $n_2 = 55$, we have $n_3 = 34$, $n_4 = 21$, $n_5 = 13$, $n_6 = 8$, $n_7 = 5$, $n_6 = 3$, $n_7 = 2$, $n_8 = 1$, $n_9 = 0$. Phew, $\gcd(89, 55) = n_8 = 1$.

Definition 1.16. If m, n are integers, we say that m and n are coprime or relatively prime to each other if $\gcd(m, n) = 1$.

Theorem 1.17 (Bezout's Theorem). *Suppose a, b are integers and $d = \gcd(a, b)$. Then there exist integers x, y such that $ax + by = d$. In particular, if a and b are relatively prime, then some integer linear combination of a and b is 1. Indeed, for $m \in \mathbb{Z}$, the equation $aX + bY = m$ is solvable with $X, Y \in \mathbb{Z}$ if and only if $d|m$.*

Sketch of Proof. The integers x, y can in fact be found via the repeated application of the Euclidean algorithm we described for computing $\gcd(a, b)$. Recall that we put $n_1 = \max(a, b)$, $n_2 = \min(a, b)$ and define recursively n_{j+1} to be the remainder of n_{j-1} divided by n_j for $j \geq 2$, viz. $n_{j-1} = q_j n_j + n_{j+1}$. Then $\gcd(a, b) = n_{s-1}$ where $n_s = 0$ (with s minimal for this property). From $n_{s-3} = q_{s-2}n_{s-2} + n_{s-1}$, we climb one level higher to $n_{s-1} = n_{s-3} - q_{s-2}n_{s-2} = n_{s-3} - q_{s-2}(n_{s-4} - n_{s-3}q_{s-3})$, and so on until we obtain an expression $n_{s-1} = xn_1 + yn_2$ for some integers x, y. Once we have $x, y \in \mathbb{Z}$ with $ax + by = d$ where $d = \gcd(a, b)$, then for any multiple m of d, say $m = kd$, we have $aX + bY = m$ for $X = kx$ and $Y = ky$. On the other hand, suppose $aX + bY = m$ with integers X, Y. We want to show that then m is a multiple of d, so let us divide and see: we have $m = qd + r$ for integers q, r where $0 \leq r < d$. By multiplying $ax + by = d$ by q, we find $axq + byq = m - r$. We subtract this from $aX + bY = m$ to find $a(X - xq) + b(Y - yq) = r$. Since $d|a$ and $d|b$, we conclude that $d|r$, which, when combined with the inequality $0 \leq d < r$ gives $r = 0$, i.e. $d|m$ as desired. □

Remark. We should note the following important interpretation of the theorem. The set of $\mathbb{Z}$-linear combinations of a and b is exactly the set of $\mathbb{Z}$-multiples of their greatest common divisor, i.e. we have an equality of sets

$$\{aX + bY \mid X, Y \in \mathbb{Z}\} = \{kd \mid k \in \mathbb{Z}\}.$$

Even more briefly, one can write $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$ where $d = \gcd(a, b)$. Later when you study rings (in Math 412), you will come to interpret this statement as “The ideal generated by a and b is principal, generated by $\gcd(a, b)$.”

Example 1.18. Determine $\gcd(200, 126)$ and express it as a linear combination of these integers. We write

$$\begin{array}{rcll}
200 & = & 126 + 74 & n_3 = 74 \\
126 & = & 74 + 52 & n_4 = 52 \\
74 & = & 52 + 22 & n_5 = 22 \\
52 & = & 2 \cdot 22 + 8 & n_6 = 8 \\
22 & = & 2 \cdot 8 + 6 & n_7 = 6 \\
8 & = & 6 + 2 & n_8 = 2 \\
6 & = & = 3 \cdot 2 & n_9 = 0.
\end{array}$$

Thus, $n_8 = 2 = \gcd(200, 126)$. Reversing the steps, we have

$$\begin{aligned}
2 &= 8 - 6 \\
&= 8 - (22 - 2 \cdot 8) \\
&= -22 + 3 \cdot 8 \\
&= -22 + 3(52 - 2 \cdot 22) \\
&= 3 \cdot 52 - 7 \cdot 22 \\
&= 3 \cdot 52 - 7(74 - 52) \\
&= -7 \cdot 74 + 10 \cdot 52 \\
&= -7 \cdot 74 + 10(126 - 74) \\
&= 10 \cdot 126 - 17 \cdot 74 \\
&= 10 \cdot 126 - 17(200 - 126) \\
&= 27 \cdot 126 - 17 \cdot 200.
\end{aligned}$$

There is a nice method, advocated by W.A. Blankinship (*Amer. Math. Monthly, 1963*), for keeping track of the straightforward but somewhat messy book-keeping of the above algorithm. It produces $\gcd(n_1, n_2)$ and the "Bezout numbers" x, y such that $xn_1 + yn_2 = \gcd(n_1, n_2)$ all in one shot. Namely, to find $\gcd(n_1, n_2)$, we write them in a column next to the 2×2 identity matrix, then we do the usual operations for finding $n_3, n_4, \ldots$ but apply each operation to the whole row. We stop when we reach a row that begins with 0. The penultimate row will then be d, x, y where $d = \gcd(n_1, n_2)$ and $d = xn_1 + yn_2$! Instead of giving a formal algorithm (and proving that it does what we say), we will be satisfied with reworking the above example with Blankinship as our guide.

Example 1.19. To find $\gcd(200, 126)$, we follow the same steps as before, but carry the algebra to the entire row each time:

$$\begin{array}{crr}
200 & 1 & 0 \\
126 & 0 & 1 \\
74 & 1 & -1 \\
52 & -1 & 2 \\
22 & 2 & -3 \\
8 & -5 & 8 \\
6 & 12 & -19 \\
2 & -17 & 27 \\
0 & 63 & -100.
\end{array}$$

We read off that $-17 \cdot 200 + 27 \cdot 126 = 2$. We also can read off $6 = 12 \cdot 200 - 19 \cdot 126$ etc. in case we wanted to. Note that $0 = 63 \cdot 200 - 100 \cdot 126$, in other words, the sixty-third multiple of 200 is also the hundredth multiple of 126, and so this number, $63 \cdot 200 = 100 \cdot 126 = 12600$ is a common multiple of 200 and 126. Are you thinking what I'm thinking? This must be the *least* common multiple of 200 and 126! Yes, that is true.

Remark. If you are familiar with row operations on matrices, you will note that the sequence of moves in the Blankinship algorithm is nothing more than that. I leave it as a challenge to the interested reader to investigate (and prove if true) whether the last row of the Blankinship algorithm will always display $0\ r\ s$ where $|rn_1| = |sn_2| = \operatorname{lcm}(n_1, n_2)$.

The Bezout theorem has a bunch of important and useful consequences.

Theorem 1.20. *If p is a prime and $p|ab$ where $a, b \in \mathbb{Z}$, then $p|a$ or $p|b$.*

Proof. Let us write $ab = pk$ for some $k \in \mathbb{Z}$. If a and b are both divisible by p, then we are done. So, let us assume one of them is not divisible by p, say b. Then by Bezout's theorem, there exist $x, y \in \mathbb{Z}$ such that $bx + py = 1$. Multiplying this last equation by b, we find $abx + apy = a$, or $p(k + ay) = a$, so $p|a$. □

Corollary 1.21. *If $n \geq 1$ and $m_1, \cdots, m_n \in \mathbb{Z}$ are n integers whose product is divisibe by p, then at least one of these integers is divisible by p, i.e. $p|m_1 \cdots m_n$ implies that then there exists $1 \leq j \leq n$ such that $p|m_j$.*

Proof. The proof is by induction on n, and is left as an exercise. □

Corollary 1.22. *For $a, b, c \in \mathbb{Z}$, if $a|bc$, and $\gcd(a, b) = 1$, then $a|c$.*

Proof. We use Bezout to write $ax + by = 1$ with $x, y \in \mathbb{Z}$. We multiply this by c to get $axc + bcy = c$, then note that $a|axc$ and $a|bcy$, so $a|axc + bcy = c$. □

Another consequence of the Bezout theorem is the following. Let's give it a fanciful name in the hope that you will remember its statement. It will be extremely useful to you when you study group theory.

Theorem 1.23 (The Supremacy of gcd and lcm). *Suppose $a, b \in \mathbb{Z}$. Every common multiple of a and b is a multiple of their least common multiple $\operatorname{lcm}(a, b)$ and every common divisor of a and b is a divisor of their greatest common divisor $\gcd(a, b)$. In other words,*

$$\begin{aligned} a|c, b|c &\implies \operatorname{lcm}(a, b)|c \\ d|a, d|b &\implies d|\gcd(a, b). \end{aligned}$$

Proof. Let $l = \operatorname{lcm}(a, b)$ and $g = \gcd(a, b)$. First, let's show that $a|c, b|c \Rightarrow l|c$. We may write $c = as$ and $c = bt$ for integers s, t. We want to show that c divided by l gives remainder 0, so let's divide and see! We have $c = lq + r$ for some integer q and some r satisfying $0 \leq r < l$. We have $c = at = lq + r$ so $r = at - lq$. Since l is a multiple of a, we then have $a|r$. Similarly, $c = bu = lq + r$ so $r = bu - lq$ is a multiple of b. Thus, r is a common multiple of a and b. But $0 \leq r < l$ and l is the least (positive!) common multiple of a and b so r cannot be positive. Thus $r = 0$, i.e. l divides c.

Now let's show that $d|a, d|b \Rightarrow d|g$. We may write $a = de$ and $b = df$ with $e, f \in \mathbb{Z}$ (by assumption), and $g = ax + by$ for $x, y \in \mathbb{Z}$ (by Bezout). Assembling all of this together, we get $g = dex + dfy = d(ex + fy)$, hence $d|g$. □

Now let us state and prove the Fundamental Theorem of Arithmetic. It says that, except for the way the prime factors are ordered, how a number breaks up into prime factors is unique.

Theorem 1.24 (The Fundamental Theorem of Arithmetic). *If $n \in \mathbb{N}$, then there is a unique function $e_n : \mathbf{P} \to \mathbb{Z}_{\geq 0}$ from the set of all primes $\mathbf{P}$ to the set of non-negative integers such that*

$$n = \prod_{p \in \mathbf{P}} p^{e_n(p)}.$$

The function e_n vanishes on all but finitely many primes.

Proof. We have already shown in Theorem 1.10 that every integer > 1 is a product of primes (and 1 is an "empty" product of primes, i.e. the function e_0 is just the function that takes the value 0 at every prime). To show uniqueness, let us proceed by contradiction (hoping to use the well-ordering principle once again). So, we suppose that there exist positive integers $n > 1$ that admit at least two distinct factorizations. By the well-ordering principle, there exists a least such integer, let us call it m. Thus, there exist two factorizations, $m = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$, where the p_i, q_j are all primes, not necessarily distinct, ordered so that $p_1 \leq p_2 \leq \ldots \leq p_r$ and $q_1 \leq q_2 \leq \ldots \leq q_s$. By assumption, the lists $p_1, \ldots, p_r$ $q_1, \ldots, q_s$ are not identical. We can assume without loss of generality[3] that $p_1 \leq q_1$. By Corollary 1.21, $p_1 | q_i$ for some $1 \leq i \leq s$. Since q_i and p_1 are both primes, we then have $p_1 = q_i$. So, $p_1 \leq q_1 \leq q_i = p_1$, so $p_1 = q_1$. Letting $m' = m/p_1$, we have, $m' = p_2 \cdots p_r = q_2 \cdots q_s$. Now these two factorizations must be distinct, since the two distinct factorizations of m are gotten by including the equal prime factors p_1 and q_1 at the beginning of each one. Thus, $0 < m' < m$ and m' has two distinct factorizations, contradicting the fact that m is the least positive integer admitting two distinct factorizations. This contradiction completes the proof. □

To compute $\operatorname{lcm}(m, n)$, one can compute $\gcd(m, n)$ and then use part (c) of the following fact.

Theorem 1.25. *Suppose $m, n \geq 1$ and*

$$m = \prod_{p \in \mathbf{P}} p^{e_m(p)}, \qquad n = \prod_{p \in \mathbf{P}} p^{e_n(p)}.$$

Then

(a)

$$\gcd(m, n) = \prod_{p \in \mathbf{P}} p^{\min(e_m(p), e_n(p))}.$$

(b)

$$\operatorname{lcm}(m, n) = \prod_{p \in \mathbf{P}} p^{\max(e_m(p), e_n(p))}.$$

(c) If $m, n \geq 1$, then $\operatorname{lcm}(m, n) \cdot \gcd(m, n) = mn$.

Proof. We leave the proof to the interested reader. □

2. Some more number theory

One of the biggest mysteries in number theory is the following problem:

Major Problem. Explain the distribution of prime numbers on the number line.

If we list the primes in order, then it becomes apparent fairly quickly that they start to "thin out." In other words, if you take an interval of length N for a large but fixed N,

[3] This oft-quoted phrase warns the reader that the author is about to make an assumption, but that this assumption is not central to the validity of the proof. Without the assumption, a simple and obvious modification or repetition of the argument can be made to account for all possible cases. For instance, in this case, if it happens that $q_1 \leq p_1$, then we simply repeat the argument, replacing all the q's by p's and vice versa.

then look at N consecutive positive integers, starting with $a+1$, then the chances that this interval $[a+1, a+N]$ contains a prime goes to zero as a goes to infinity. Here is a "movie" of this phenomenon: If you take a "window" of fixed width and shift it to the right, the chances that you catch a prime for any given frame goes to zero as you shift to the right.

In a sense, you should expect that the primes are "outmuscled" by the composites, because everytime you have a bunch of primes, you can combine them in many ways in order to make composites, but there is only one way to make a prime. In particular, in one of the homework problems, you will show that no matter how large N is, as you shift to the right, you are bound to hit a frame with no primes in it. Here is another way in which composites "outmuscle" the primes.

Example 2.1. A sequence $x_0, x_1, x_2, \cdots$ in $\mathbb{Z}$ is called *arithmetic* if there exists an integer a (called the *addend*) such that $x_{n+1} - x_n = a$ for all $n \geq 1$. Equivalently, $x_n = x_0 + na$. Show that any arithmetic sequence in $\mathbb{Z}$ with non-zero addend contains infinitely many composites.

Here is a proof. Suppose $(x_n)_{n\geq 0}$ is an arithmetic sequence with addend a. If all the x_n are composite, we are certainly done! If not, let $p = x_0 + ma$ be prime for some $m \geq 0$. We claim that if $n = m + kp$, where $k \geq 1$, then x_n is composite. Once we prove the claim, we are done, of course. To prove the claim, note first that x_n is divisible by p because

$$x_n = x_0 + an = x_0 + a(m + kp) = x_0 + am + akp = p + akp = p(1 + ak).$$

Note that $x_n = p(1 + ak) > p$ for $k \geq 1$, hence x_n is divisible by p and greater than p hence it is composite, proving the claim.

On the other hand, primes are "persistent" in some ways. For instance, as we proved, there are infinitely many of them! A much more subtle and powerful theorem, first formulated by Lagrange, and finally proved by Peter Gustav Lejeune Dirichlet in 1837, says that in any arithmetic progression that has the potential of having infinitely many primes does have infinitely many primes.

Theorem 2.2 (Dirichlet's Theorem on Primes in Arithmetic Progressions)**.** *If* $x_0, a \in \mathbb{N}$ *and* $\gcd(a, x_0) = 1$*, then the arithmetic sequence* $x_0, x_0 + a, x_0 + 2a, \ldots, x_0 + an, \ldots$ *contains infinitely many primes.*

Note that the assumption $\gcd(x_0, a) = 1$ is needed, because otherwise all the elements in the sequence are divisible by $d > 1$ where $d = \gcd(x_0, a)$. Dirichlet's ideas for proving this theorem consitute the foundations of an entire branch of modern mathematics known as "analytic number theory."

Another "prime persistence" theorem, due to Chebyshev, is known as "Bertrand's Postulate." It says that for $n \geq 1$, the interval $(n, 2n]$ contains at least one prime. Here is an unsolved problem.

Question 2.3. Is it true that for all large enough n, (say $n \geq 117$), the interval $[n, n + \sqrt{n}]$ contains a prime? (It is believed that the answer is "yes" but no proof or counterexample is known at present).

A spectacular and recent "prime persistence" theorem is the following.

Theorem 2.4 (Peter Green and Terence Tao, 2004)**.** *Given* $N \geq 1$*, there exists integers* $x_0, a \in N$ *such that* $x_0 + a, x_0 + 2a, \ldots, x_0 + Na$ *are all primes. In other words, there are arbitrarily long arithmetic progressions of primes.*

See `http://arxiv.org/abs/math.NT/0404188` for their paper. You may not understand much, but you'll get a glimpse of what a mathematical "preprint" (an article in pre-published form) looks like. One of the most exciting aspects of their proof is that it uses techniques of "ergodic theory," a branch of "analysis" (calculus).

The fact that the study of smooth functions $\mathbb{R} \to \mathbb{R}$ should say anything about arithmetic properties of whole numbers might be surprising at first, but this tradition actually goes way back to Leonhard Euler at least who gave a proof of the infinitude of primes based on the fact that the harmonic series

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots$$

diverges! Euler's observation led Georg Bernhard Riemann to the study of the function

$$\zeta(x) = 1 + \frac{1}{2^x} + \frac{1}{3^x} + \cdots + \frac{1}{n^x} + \cdots$$

which Euler had introduced, but which we now call the **Riemann Zeta Function**. Riemann observed that the *analytic* properties of this function reveal some deep *arithmetic* facts about the distribution of primes on the number line! The connection between them is sealed by the Euler Product Formula:

$$\zeta(x) = \prod_{p \in \mathbf{P}} \frac{1}{1 - \frac{1}{p^x}}$$

which in turn holds because of the Fundamental Theorem of Arithmetic. In 1859, Riemann outlined a program, completed by de la Vallée-Poussin and Hadamard independently in 1896, for proving a conjecture of Gauss which we now call the Prime Number Theorem. To state it, let us define the Prime Counting Function $\pi(x) = |\{p \in \mathbf{P} \mid p \leq x\}|$ which counts the number of primes in the interval $[1, x]$. Up close, this function is quite choppy, as it jumps by 1 everytime it encounters a prime. But if you look at its graph on a very large interval, it looks remarkably smooth. So the question is: Is there a nice simple continuous function whose graph approaches the graph of $\pi(x)$ as x tends to infinity? The answer is "Yes," and one function which fits the bill is $x/\ln(x)$.

Theorem 2.5 (The Prime Number Theorem). *We have*

$$\lim_{x \to \infty} \frac{\pi(x)}{x/\ln(x)} = 1.$$

The theorem says that $\pi(x)$ and $x/\ln(x)$ are about the same size. For example, in 1959, Derrick Lehmer (my mathematical grandfather) calculated on his super-duper computer that $\pi(10^{10}) = 455052511$,i.e. is about 455 million. Let us compare that to $10^{10}/\ln(10^{10}) \approx 434294482$ or about 434 million. I wonder whether you are impressed by this or not. On the one hand, we are off by about 21 million primes! On the other hand, calculating $10^{10}/\ln(10^{10})$ takes just a second whereas counting how many primes there are up to 10^{10} is serious business. In retrospect, 21 million primes out of 455 million is only about a 4.5% error. Not too bad at all! Nonetheless, one would like to understand how much the error $\pi(x) - x/\ln(x)$ is, or at least put a cap on this error. Riemann's method does give us a bound on this error, but the bound is MUCH bigger than the actual errors we observe. Riemann has an explanation for that too: He thinks it is highly likely that the roots of his function (not just for x in $\mathbb{R}$ for complex numbers x) all lie on a certain line. To find out whether this is true or not is one of the hottest problems in Mathematics. It is known as The Riemann Hypothesis, the subject of various recent popular books.

3. Problems

1. Suppose $a, b, c \in \mathbb{Z}$.
(a) Show that if $a|b$ and $c \neq 0$, then $ca|cb$.
(b) Show that if $a|b$ and $b|c$, then $a|c$.
(c) Show that if $a|b$ and $a|c$, then $a|(mb + nc)$ for all $m, n \in \mathbb{Z}$.

2. Show that there are arbitrarily long sequences of consecutive integers containing no primes. In other words, show that given an integer $N \geq 1$, there exists an integer a such that $a + 1, a + 2, \ldots, a + N$ are all composites. Hint: try $a = N! + 1$. Look for an "obvious" divisor of $a + 1$, an "obvious" divisor of $a + 2$ etc.

3. Suppose a, b, n are integers, $n \geq 1$ and $a = nd + r$, $b = ne + s$ with $0 \leq r, s < n$, so that r, s are the remainders for $a \div n$ and $b \div n$, respectively. Show that $r = s$ if and only if $n|(a - b)$. [In other words, two integers give the same remainder when divided by n if and only if their difference is divisible by n.]

4. If $n \geq 1$ and $m_1, \cdots, m_n \in \mathbb{Z}$ are n integers whose product is divisibe by p, then at least one of these integers is divisible by p, i.e. $p|m_1 \cdots m_n$ implies that then there exists $1 \leq j \leq n$ such that $p|m_j$. Hint: use induction on n.

5. (a) Calculate $\gcd(315, 168)$ using the Euclidean algorithm, then use this information to calculate $\operatorname{lcm}(315, 168)$. Determine integers x, y such that $315x + 168y = \gcd(315, 168)$. You may use the Blankinship version of the Bezout algorithm if you wish. Now obtain the prime factorizations of 315 and 168 to double-check your computation of the gcd and lcm of 315 and 168.
(b) Calculate $\gcd(89, 148)$ using the Euclidean algorithm.

6. (a) Show that if $n > 1$ is composite, then there exists d in the range $1 < d \leq \sqrt{n}$ such that $d|n$. (Hint: you might want to use proof by contradiction).
(b) Use (a) to show that if n is not divisible by any integers in the range $[2, \sqrt{n}]$, then n is prime.
(c) Use (b) to show that if n is not divisible by any **primes** in the range $[2, \sqrt{n}]$, then n is prime.
(d) Use the procedure in (c) to verify that 229 is prime.
(e) Suppose you write down all the primes from 2 to n. We know that 2 is a prime so we circle it and cross out all other multiples of 2. The next uncrossed number is 3 and we claim that 3 therefore must be prime. Explain why. Now cross out all the multiples of 3. The next uncrossed number is 5 so we claim it must be a prime. We continue in this fashion until we get to $\sqrt{n}$. Explain why all the remaining numbers are prime. Carry out this procedure for $n = 100$ to find all the primes less than 100. This is called the Eratosthenes sieve. (You may want to write them in 10 rows of 10 numbers each).

7. (a) Prove that if $n \in \mathbb{N}$, then $\gcd(n, n + 1) = 1$.
(b) Is it possible to choose 51 integers in the interval $[1, 100]$ such that no two chosen numbers are relatively prime? [i.e. is there a subset $S \subset \{n \in \mathbb{N} \mid 1 \leq n \leq 100\}$ with

$|S| = 51$ such that $m, n \in S \Rightarrow \gcd(m, n) > 1$?] Prove that your answer is correct. (Hint: If you get stuck, recall that an often useful problem-solving strategy is to attempt a simpler problem first, so think about 6 integers in $[1, 10]$ for example).

8. Show that for $n \geq 1$, in any set of $2^{n+1} - 1$ integers, there is a subset of exactly 2^n of them whose sum is divisible by 2^n. (Hint: use ordinary induction on n).

9. Suppose x is a real number such that $x + 1/x$ is an integer. Show that $x^n + 1/x^n$ is also an integer for all $n \geq 1$. (Hint: Use complete induction on n).

10. Here is a "proof" by complete induction that all Fibonacci numbers are even! Your job is to explain the error in the argument.

For $n \geq 0$, let $P(n)$ be the statement that F_n is even. We will prove $P(n)$ by complete induction on n. We check the base case, $P(0)$: $F_0 = 0$ is even. Now we move to the induction step: We must show that if $P(j)$ holds for $0 \leq j \leq n$, then $P(n)$ holds. Well, if $P(j)$ holds for $0 \leq j \leq n$, then $F_{n+1} = F_{n-1} + F_n$ is even because F_{n-1} and F_n are even by $P(n-1)$ and $P(n)$, respectively. By Complete Induction, therefore, F_n is even for all $n \geq 0$.

4. Extra Credit

A. Let $a_1, a_2, \ldots, a_{100}$ be a sequence of length 100 in $\mathbb{N}$. Show that there is a non-trivial subsequence of this sequence whose sum is divisible by 100. In other words, show that there exists an integer $N \geq 1$ and integers $1 \leq i_1 < i_2 < \cdots < i_N \leq 100$ such that $a_{i_1} + a_{i_2} + \cdots + a_{i_n}$ is divisible by 100.

Hint: Use the pigeon-whole principle as applied to the remainders of the numbers when divided by 100.

B. It is a fact, due to Chebyshev, that for any integer $n \geq 1$, there exists a prime in the interval $(n, 2n]$. Use this fact to prove that the *harmonic numbers* defined by

$$H_k = \sum_{j=1}^{k} \frac{1}{j} = 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{k},$$

are not integers for $k > 1$.

C. Recalling the Fibonacci numbers from the previous homework, show that

$$F_n = F_k F_{n-k} + F_{k-1} F_{n-k-1} \qquad \text{for } 1 \leq k \leq n-1.$$

5. Super Extra Credit

D. Let $a_1, a_2, \ldots, a_{51}$ be integers with $1 \leq a_i \leq 100$ for all $1 \leq i \leq 51$. Prove that there exists $i \neq j$ such that $a_i | a_j$.

6. Super Duper Extra Credit

E. Let $n \geq 1$ be a positive integer. Suppose you have $2n+1$ not necessarily distinct positive integers such that whenever one of the numbers is removed, the remaining $2n$ numbers can be divided into two groups of size n that add up to the same number. Show that the numbers are all the same.

To state this more formally, let $S = \{1, 2, 3, \dots, 2n, 2n+1\}$. Suppose $f : S \to \mathbb{N}$ is a map such that for all $x \in S$, there exist sets $T, U \subset S \setminus \{x\}$ such that $T \cap U = \emptyset$, $|T| = |U| = n$, and $\sum_{t \in T} f(t) = \sum_{u \in U} f(u)$. Show that f is a constant function i.e. for all $s_1, s_2 \in S$, $f(s_1) = f(s_2)$.

Hint: It is relatively easy to prove that all the numbers have the same parity. Is this helpful at all?