Math 25 — Assignment 1 (Solutions)

Due Tuesday, September 27, *beginning of class*.

1. Prove that:

   (a) If $a \mid b$ and $b \mid c$ then $a \mid c$.

   (b) If $a \mid b$ and $c \mid d$ then $ac \mid bd$.

   (c) If $m \neq 0$ then $a \mid b$ if and only if $ma \mid mb$.

   (d) If $d \mid a$ and $a \neq 0$ then $|d| \leq |a|$.

   Solution: In the following we shall denote by x, y the appropriate integers used in the definition of divisibility.

   (a) Write $b = xa$ and $c = yb$. Then $c = xya$, so $a \mid c$.

   (b) Write $b = xa$ and $d = yc$. Then $bd = xy \cdot ac$, so $ac \mid bd$.

   (c) Notice that for $m \neq 0$, we have $b = xa$ iff $mb = mxa$. Thus the claim.

   (d) (This was done in class.) Write $a = xd$. Since $a \neq 0$, we have $d \neq 0$. We have $|x| \geq 1$ for all $x \in \mathbb{Z}$, so $|a| = |x| \cdot |d| \geq |d|$.

2. Let a, b, e be positive integers. If $e \mid a$ and $e \mid b$, prove that $e \mid \gcd(a, b)$.

   Solution:

   From Bezout's identity, there exist integers x, y such that

   $$ax + by = \gcd(a, b).$$

   Because e is a common divisor of a, b, it follows from Theorem 1.3 of the book that $e \mid \gcd(a, b)$. (That is, e divides any integer linear combination of a and b.)

3. Let a, b be integers with $b > 0$. Prove that there exist unique integers q, r such that

   $$a = qb + r$$

   where $-\frac{b}{2} < r \leq \frac{b}{2}$. Additionally, prove that there exist unique integers q, r such that

   $$a = qb + r$$

   where $-b < r \leq 0$.

   Solution:

   Set $\beta := \lceil b/2 \rceil - 1$. Note $-\frac{b}{2} < -\beta$ and $b - \beta \leq \frac{b}{2}$. From the Division Algorithm, there are unique integers q, r' such that

   $$(a + \beta) = qb + r'$$

   and $0 \leq r' < b$. Thus, given any integer a, there are unique integers q, r' such that

   $$a = qb + (r' - \beta).$$

   Set $r = r' - \beta$. We have that $\frac{b}{2} < r \leq \frac{b}{2}$. It is clearly the unique remainder in this range, since subtraction-by-β is a bijection on $\mathbb{Z}$ which sends $\{0, \ldots, b-1\}$ to $\{x \in \mathbb{Z} : \frac{b}{2} < x \leq \frac{b}{2}\}$.

Similarly, from the division algorithm, there are unique integers x, r'' such that

$$(a+b-1) = xb + r''.$$

So

$$a = xb + (r'' - b + 1).$$

Setting $r = r'' - b + 1$, we have $-b < r \leq 0$. As before we see r is the unique with regard to this property.

4. Given an element $\alpha = \frac{c}{d} \in \mathbb{Q}$, we can write the Hirzebruch-Jung continued fraction expansion as

$$\alpha = a_0 - \cfrac{1}{a_1 - \cfrac{1}{a_2 - \cfrac{1}{\ddots - \cfrac{1}{a_k}}}}$$

for some unique finite list of integers $a_0, a_1, \ldots, a_k$ such that $a_j > 1$ for each $1 \leq j \leq k$. (In the case $\alpha \in \mathbb{Z}$, we set the continued fraction expansion to be $\alpha = a_0$.)

(a) Explain how to compute a_0. (Hint: $|\alpha - a_0| < 1$. See part (d).)

(b) Explain how to compute the sequence $a_0, \ldots, a_k$. Comment briefly on how this is related to the Euclidian algorithm.

(c) Prove for all $n > 1$ that

$$\frac{n+1}{n} = 2 - \cfrac{1}{2 - \cfrac{1}{2 - \cfrac{1}{\ddots - \cfrac{1}{2}}}}$$

for some number of 2's.

(d) (Advanced topics[1]) Prove that $|\alpha - a_0| < 1$ in any Hirzebruch-Jung continued fraction expression. Use this to prove that the Hirzebruch-Jung continued fraction expansion is unique, provided it exists.

Solution:

(a) We claim that a_0 must be the minimal element of $\{d \in \mathbb{Z} : \alpha \leq d\}$. From part (d) we have $|\alpha - a_0| < 1$ for any valid a_0. Notice that the interval $(\alpha - 1, \alpha + 1)$ is of length 2, so:

- either $\alpha \notin \mathbb{Z}$ and there are two integers x, y in this interval, which must satisfy $x < \alpha < y$, or,
- $\alpha \in \mathbb{Z}$, in which case α is the unique integer in $(\alpha - 1, \alpha + 1)$.

In the second case, we have that $\alpha = a_0$ by definition.

Otherwise, we are in the first case. We rule out $a_0 = x$ via contradiction. Were this the case, then

$$0 > \frac{1}{a_0 - \alpha} = \frac{1}{x - \alpha} = a_1 - \cfrac{1}{a_2 - \cfrac{1}{\ddots - \cfrac{1}{a_k}}}.$$

We write the rightmost quantity as $a_1 - \epsilon$, which by part (d) satisfies $|\epsilon| < 1$. From the properties of Hirzebruch-Jung continued fractions, we see $a_1 > 1$. Thus $a_1 - \epsilon > a_1 - 1 > 0$, a contradiction.

Thus, as in the second case, we have that a_0 is equal to the smallest integer not smaller than α.

[1] Advanced topics questions are not counted towards the score, but I will offer feedback on your solution. They are meant to be a challenge.

(b) From part (a), and the fact that the Hirzebruch-Jung continued fraction expansion is unique, we can compute the sequence recursively using the Euclidian algorithm.

Write $\alpha = \frac{p_0}{q_0}$ in lowest terms. By Question 2, we can compute a_0, r_0 such that

$$p_0 = a_0 \cdot q_0 - r_0$$

where $0 \leq r_0 < q_0$. Note from this equation that a_0 is the smallest integer such that $\alpha \leq a_0$, as $\frac{r_0}{q_0} < 1$. If $r_0 = 0$ we stop, and otherwise

$$\alpha = a_0 - \frac{1}{(q_0/r_0)}.$$

We then compute the Hirzebruch-Jung continued fraction expansion of $\alpha_1 := q_0/r_0$. Note that this algorithm terminates, since the Euclidian algorithm terminates in a finite number of steps (alternatively, since it is given that the continued fraction expansion has finite length).

(c) We prove the claim by induction. For $n = 2$ we see that $\frac{3}{2} = 2 - \frac{1}{2}$. We assume that the result is true for some $n \geq 2$, and show this implies the result for $n + 1$.

Observe that $\frac{n+1}{n} = 1 + \frac{1}{n}$, which lies in $(1, 2)$. Thus, we compute a_0 using part (a) to see that $a_0 = 2$. Now

$$\frac{n+1}{n} = 2 - \frac{1}{\left(\frac{n}{n-1}\right)}.$$

The Hirzebruch-Jung continued fraction expansion for $\frac{n}{n-1}$ can be substituted into this expression, giving by the induction hypothesis

$$\frac{n+1}{n} = 2 - \cfrac{1}{2 - \cfrac{1}{2 - \cfrac{1}{2 - \cfrac{1}{\ddots - \cfrac{1}{2}}}}}.$$

This is of course a valid Hirzebruch-Jung continued fraction. Thus, by induction the result is proven for all n.

5. A *square-free* integer is an integer n such that $m^2 \mid n$ implies $n = 1$. That is, the only square dividing n is 1. Prove that every non-zero integer n can be written uniquely as a product $n = ab^2$ with a a square-free integer.

Solution: Let

$$n = (-1)^s \cdot \prod_{i=1}^{k} p_i^{e_i}$$

be the unique factorization of n. Let $E := \{i : 2 \mid e_i, 1 \leq i \leq k\}$ and let $N := \{1, \ldots, k\} \backslash E$. Then

$$\begin{aligned} n = (-1)^s \cdot \prod_{i \in E} p_i^{e_i} \cdot \prod_{i \in N} p_i^{e_i} &= (-1)^s \cdot \prod_{i \in E} p_i^{e_i} \cdot \prod_{i \in N} p_i \cdot \prod_{i \in N} p_i^{e_i - 1} \\ &= (-1)^s \cdot \prod_{i \in N} p_i \cdot \left(\prod_{i \in E} p_i^{e_i} \cdot \prod_{i \in N} p_i^{e_i - 1} \right) \\ &= (-1)^s \cdot \prod_{i \in N} p_i \cdot \left(\prod_{i \in E} p_i^{\frac{e_i}{2}} \cdot \prod_{i \in N} p_i^{\frac{e_i - 1}{2}} \right)^2. \end{aligned}$$

By definition of E and N, the exponents of the bracketed term are integers, so in particular the bracketed term is itself an integer. We set

$$a := (-1)^s \cdot \prod_{i \in N} p_i, \qquad b := \left(\prod_{i \in E} p_i^{\frac{e_i}{2}} \cdot \prod_{i \in N} p_i^{\frac{e_i - 1}{2}} \right).$$

Note that a is squarefree. (If p is a prime and $p|m^2$, then $p|m$, so $p^2|m^2$. Unique factorization shows that the only square dividing a is 1.) Thus we have produced a squarefree factorization.

We now prove uniqueness. Let $n = ab^2 = cd^2$ be two squarefree factorizations, with a, b as before. Then

$$acb^2 = (cd)^2 \implies ac = \left(\frac{cd}{b}\right)^2 \in \mathbb{Z},$$

so ac is a square. It is in particular positive, and the unique factorization has even exponents for each prime. In particular each prime dividing a must also divide c, so $a|c$.

Write $c = qa$. Since $ac = qa^2$ is a square, we have that q is a square. But c is squarefree, so $q = 1$ and $a = c$. This implies $b = d$, and thus that the squarefree factorization is unique.

6. (Advanced topics) Let $f(x)$ be a polynomial with non-negative integer coefficients. Classify all such f such that $f(n)$ is prime for all $n \in \mathbb{N}$.

7. (Advanced topics) Use the Prime Number Theorem and a bit of calculus to prove the following weaker form of Bertrand's Postulate:

   Proposition. There are only finitely many $n \in \mathbb{N}$ such that the interval $[n, 2n]$ does not contain a prime number.