

MATH221-001 200530 Sample Term Test 1 Solutions

Edward Doolittle

Sunday, October 2, 2005

Solutions to the last three problems have been updated.

1. (2 marks) Using a calculator, you can see that $1860/48 = 38.75$. That means the quotient should be $q = 38$. $48 \times 38 = 1824$ so the remainder should be $r = 1860 - 1824 = 36$. You should double check that $1848 = 48 \times 38 + 36$.
2. (3 marks) We use the Euclidean algorithm. Dividing again, we see that $48 = 36 \times 1 + 12$, and again we see that $36 = 12 \times 3 + 0$. Since the remainder is now 0 we stop. The greatest common divisor of 1860 and 48 is the divisor in the last division (the one with remainder 0), i.e., $\gcd(1860, 48) = 12$.
3. (5 marks) Using the division relations derived in the previous two problems,

$$12 = 48 \times 1 - 36 \times 1 \tag{1}$$

$$36 = 1860 \times 1 - 48 \times 38 \tag{2}$$

Substituting the second equation into the first we obtain

$$\begin{aligned} 12 &= 48 \times 1 - 36 \times 1 \\ &= 48 \times 1 - (1860 \times 1 - 48 \times 38) \times 1 \\ &= 48 \times 1 + 48 \times 38 - 1860 \times 1 \\ &= 1860 \times (-1) + 48 \times 39, \end{aligned}$$

so $m = -1$, $n = 39$ works.

4. (4 marks) One way to solve this problem is to notice that

$$0 = 1860 \times 48 + 48 \times (-1860) \tag{3}$$

Adding that equation to the equation

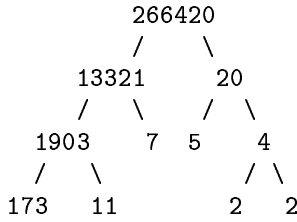
$$12 = 1860 \times (-1) + 48 \times 39 \tag{4}$$

obtained in the previous problem, we see that

$$12 = 1860 \times 47 + 48 \times (-1821) \tag{5}$$

which gives $p = 47$, $q = -1821$.

5. (3 marks) The square root of 173 is just slightly larger than 13 so we just have to try to divide 173 by the prime numbers up to and including 13, namely 2, 3, 5, 7, 11, and 13. Using a calculator, or some of the divisibility tests discussed in the lectures, you can see that none of the above primes divides evenly into 173, so 173 itself must be a prime.
6. (5 marks) Dividing first by the obvious factor of 20, and then by primes 3, 5, 7, and 11 in succession, we see that one possible factor tree for 266420 is



We know from the previous problem that 173 is prime, so we stop there. From the factor tree, we can read the prime factorization $266420 = 2^2 \times 5^1 \times 7^1 \times 11^1 \times 173^1$.

7. (5 marks) From the theorem proven in the lectures, we know that

$$d = pa + qb \tag{6}$$

for some integers p and q . On the other hand, since D is a multiple of d , we can write $D = kd$ for some integer k . Multiplying (6) through by k we obtain $D = kd = kpa + kqb = (kp)a + (kq)b$, so the equation $D = ma + nb$ is true with $m = kp$ and $n = kq$.

8. (8 marks) This problem explores the concept of division with ‘least remainder’, as opposed to the division algorithm presented in the lecture which gives ‘least nonnegative remainder’. You could work the theory for ‘least remainder’ division out from scratch the way it was done in the lectures for division with “least nonnegative remainder”. However, that would take a long time. You should instead use the results of the lectures as a starting point and work from there.

To prove the existence of q' and r' , apply the division algorithm presented in the lectures to a and b to obtain $a = bq + r$ where $0 \leq r < b$. If $r \leq b/2$, we can let $q' = q$ and $r' = r$ and we are done because we have found q' and r' such that $a = bq' + r'$ and $-b/2 < 0 \leq r' \leq b/2$.

On the other hand, if $b/2 < r < b$, then we can subtract and add b to the division relation to obtain $a = b(q+1) + (r-b)$. Since $b/2 < r < b$, subtracting b throughout that inequality gives $-b/2 < r-b < 0$. Letting $q' = q + 1$ and $r' = r - b$, we have again found q' and r' satisfying the conditions because $a = bq + r = b(q+1) + (r-b) = bq' + r'$ and $-b/2 < r' < 0 < b/2$.

Existence has been established. For uniqueness, suppose that $a = bq'_1 + r'_1 = bq'_2 + r'_2$ where $-b/2 < r'_1 \leq b/2$ and $-b/2 < r'_2 \leq b/2$. Subtracting the latter two expressions for a , we have $b(q'_1 - q'_2) = r'_2 - r'_1$. It follows that $r'_2 - r'_1$ is a multiple of b . On the other hand, consider the inequalities

$$-b/2 < r'_2 \leq b/2 \tag{7}$$

$$-b/2 < r'_1 \leq b/2. \tag{8}$$

The inequality (8) is really two separate inequalities, $-b/2 < r'_1$ and $r'_1 \leq b/2$. Multiplying each of those by -1 we obtain

$$b/2 > -r'_1$$

and

$$-r_1 \geq -b/2$$

(remember that the direction of an inequality is reversed when it is multiplied by a negative number). Putting the latter two inequalities together, we obtain

$$-b/2 \leq -r_1 < b/2. \tag{9}$$

Adding inequalities (7) and (9) we obtain

$$-b < r'_2 - r'_1 < b$$

(Why can we write ‘ $<$ ’ above instead of ‘ \leq ’?) But recall that we know that $r'_2 - r'_1$ is a multiple of b . The only multiple of b in the range between $-b$ and b (excluding those two values) is 0. So $r'_2 - r'_1 = 0$ which implies $r'_2 = r'_1$ and $b(q'_1 - q'_2) = 0$ which (since $b \neq 0$) implies $q'_1 = q'_2$. This shows that ‘least remainder’ division is unique.

9. (5 marks) In the expression $\gcd(a + b, a - b)$, subtract the second number from the first to obtain $\gcd(a + b, a - b) = \gcd(2b, a - b)$. Let $d = \gcd(2b, a - b)$. Since one of a and b is even and the other is odd, it follows that $a - b$ is odd. It follows that d cannot have a factor of 2 (if it did have a factor of 2 then $a - b$ would have to have a factor of 2, but we know $a - b$ is odd). Since d divides $2b$ and d is odd, it follows (e.g., from unique factorization) that d divides b . Therefore $d = \gcd(b, a - b)$, so $\gcd(b, a) = \gcd(b, a - b) = d = \gcd(a + b, a - b)$ and we are done.
10. (5 marks) This is actually quite easy if you have a good idea of what ‘greatest common divisor’ means. Suppose m divides n . Then $\gcd(m, n) = m$. (Why?) So, by the given result, $\gcd(f_m, f_n) = f_{\gcd(m, n)} = f_m$. It is only possible for f_m to be the greatest common divisor of f_m and f_n if f_m is in fact a divisor of f_n .
- To illustrate, take $m = 3$ and $n = 9$. Then $f_9 = 34$ is a multiple of $f_3 = 2$. Or take $m = 4$ and $n = 8$; then $f_8 = 21$ is a multiple of $f_4 = 3$. Or take $m = 5$ and $n = 10$; then $f_{10} = 55$ is a multiple of $f_5 = 5$.