Math 110 HW 1 solutions

April 18, 2013

1. Find the greatest common divisor of 1112 and 1544.

$$\begin{array}{llllr} 1544 & -1\times & 1112 & = & 432 \\ 1112 & -2\times & 432 & = & 248 \\ 432 & -1\times & 248 & = & 184 \\ 248 & -1\times & 184 & = & 64 \\ 184 & -2\times & 64 & = & 56 \\ 64 & -1\times & 56 & = & 8 \\ 56 & -7\times & 8 & = & 0 \end{array}$$

   so having run the Euclidean algorithm we find $\gcd(1112, 1544) = 8$.

2. For the value d of the greatest common divisor found in the

   first question, find all integer solutions (x, y) to the equation $1112x + 1544y = d$.

   We reuse the quotients in the first part of the algorithm, to get one solution:

$$\begin{array}{lllll} 8 & = & 64 - 56 & & \\ 8 & = & 64 - (184 - 2*64) & = & 3*64 - 184 \\ 8 & = & 3(248 - 184) - 184 & = & 3*248 - 4*184 \\ 8 & = & 3*248 - 4*(432 - 248) & = & 7*248 - 4*432 \\ 8 & = & 7*(1112 - 2*432) - 4*432 & = & 7*1112 - 18*432 \\ 8 & = & 7*1112 - 18*(1544 - 1112) & = & 25*1112 - 18*1544. \end{array}$$

   Algebraic method to find more solutions: Then we note that $1544/8 = 193$ and $1112/8 = 139$, so in particular $139 \times 1544 - 193 \times 1112 = 0$ which is the smallest pair of positive integers giving that solution, because it is the least common multiple minus itself.

   Given two solutions, $1112x + 1544y = 8$ and $1112w + 1544z = 8$, we can subtract them to find $1112(x - w) + 1544(y - z) = 0$, which is an integer solution to the equation above. Therefore $x - w = 139n$ for some integer n, and $y - z = 193n$.

Thus, the set of all possible solutions is $8 = (25 + 193n) \times 1112 - (18 + 193n) \times 1544$, for all integers n.

Geometric method to find more solutions:

The set of points (x, y) where $1112x + 1544y = 8$ is a line, and we want to find points on that line whose coordinates are integers. We have one, the point $(25, -18)$. Now, the slope is $-1112/1544 = -139/193$. So if we change x by an integer amount m, y will be changed by $-139m/193$, which is an integer only if 193 divides m. Write $m = 193n$ for an integer n, and we see that again the set of all possible solutions is $8 = (25 + 193n) \times 1112 - (18 + 193n) \times 1544$.

3. Find all solutions of the congruences $12x \equiv 28 \mod 236$ and $12y \equiv 30 \mod 236$.

   First note that 236 factors as $59 * 4$. So we wish to find x that solves $12x \equiv 0 \mod 4$, and $12x \equiv 28 \mod 59$. The first equation is true for every x.

   For the second, let us take a few multiples of 12, mod 59: $12, 24, 36, 48, 1-$ and stop because knowing that $12*5 = 1$ allows us to solve everything else. Now $12*(5*28) \equiv 28 \mod 59$, and so a solution is $x = 5*28 = 140 \equiv 22 \mod 59$.

   If we try this x as a solution we have $12 * 22 = 264 \equiv 28 \mod 236$ as desired.

   Now we wish to find y that solves $12y \equiv 2 \mod 4$ and $12y \equiv 30 \mod 59$. Since the equation $12y \equiv 2 \mod 4$ is equivalent to $0y \equiv 2 \mod 4$ and has no solutions, we conclude that there are no solutions in this case.

4. Find a multiplicative inverse of $7 \mod 30$.

   There are several ways to do this, straightforward ones being multiples of 7 and powers of 7. I'll go with powers of 7.

$$\begin{aligned} 7^2 = 49 \equiv 19 &\mod 30 \\ 7^3 \equiv 19 \times 7 \equiv 133 \equiv 13 &\mod 30 \\ 7^4 \equiv 13 \times 7 \equiv 91 \equiv 1 &\mod 30. \end{aligned}$$

   So we find that 13 is a multiplicative inverse of 7, modulo 30.

5. Let p be a prime number and n a positive integer. Show that the largest power of p which divides $n!$ is given by

$$\sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor.$$

   Since $n!$ is the product of the integers from 1 to n, let's first count how many of those integers are divisible by p. That is the multiples of p; there are n/p of them rounded down to the nearest integer, which is to say, $k_1 = \lfloor \frac{n}{p} \rfloor$.

Next, let's count how many of those integers are divisible by p^2. Again that is the multiples of p^2, and there are $k_2 = \lfloor \frac{n}{p^2} \rfloor$.

Similarly counting the number of integers that are divisible by p^3 and calling that number k_3, and so on, eventually $k_i = 0$ for all i after some number. So we have a sequence $k_1, k_2, \ldots$ of which all but finitely many terms are 0. Let K be the sum $\sum_{i=1}^{\infty} k_i$, which is the sum in the problem statement, and which is a finite number.

Therefore, considering all the powers of p contributed to $n!$ by multiples of p, they sum up to K, which means the number p^K divides $n!$. The question is, is K the largest possible exponent here?

At this point it becomes important that p is prime: for any two numbers b, c, if $p|bc$ then $p|b$ or $p|c$. From that statement one may deduce that if $p^m|bc$, then $p^i|b$ and $p^j|c$ for nonnegative integers i, j such that $i + j \geq m$. Also, both statements apply not only to two integers b, c but to any product of finitely many integers.

Thus if p^{K+1} divides $n!$, then among the integers from 1 to n there are exponents of p which sum up to at least $K + 1$. Since this is false, we know p^{K+1} does not divide $n!$, so K is the largest exponent for which $p^K|n!$, q.e.d.

6. Prove that the binomial coefficient $\binom{2n}{n=\frac{(2n)!}{n!n!}}$ divides the product

$$\prod_p p^{\lfloor \log_p(2n) \rfloor}$$

where the product is taken over all primes p.

First, note that $\lfloor \log_p(2n) \rfloor$ is the exponent of the largest possible power of p that is $\leq 2n$. So the expression in the product, $p^{\lfloor \log_p(2n) \rfloor}$, is just the largest possible power of p that is $\leq 2n$.

For a given p, suppose $p^k \leq 2n$ and $p^{k+1} > 2n$. Then let us see how many powers of p divide $n! * n!$, which would be given by

$$S_1 = 2 \sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor.$$

The number of powers of p that divide $(2n)!$ is

$$S_2 = \sum_{i=1}^{\infty} \left\lfloor \frac{2n}{p^i} \right\rfloor.$$

and the problem statement is equivalent to proving that $S_2 \leq S_1 + k$.

The last nonzero number in the second sum is $a = \lfloor \frac{2n}{p^k} \rfloor$ and in the first sum we have the corresponding term $2\lfloor \frac{n}{p^k} \rfloor = 2\lfloor \frac{a}{2} \rfloor$. We can see that $a - 2\lfloor \frac{a}{2}$ is equal to 0 or 1 depending on whether a is even or odd. But this argument holds true also for the comparison of $\lfloor \frac{2n}{p^i} \rfloor$ and $2\lfloor \frac{n}{p^i} \rfloor$ for $i = 1, \ldots k - 1$.

Each of these comparisons differs by 0 or 1, thus we have $S_2 \leq S_1 + k$.