MAT 311: Number Theory
Spring 2006

HW3 - Solutions

1. (Davenport, pp.217, ex. 1.20) We will find all integral solutions of the equation 113x - 355y = 1. By Euclid’s theorem, this equation has a solution since (113, 355) = 1. Indeed, by Euclid’s algorithm, we get

\[ 355 = 113 \cdot 3 + 16 \]
\[ 113 = 16 \cdot 7 + 1 \]
\[ 16 = 1 \cdot 16. \]

So, (113, 355) = 1. Moreover, this algorithm (traversing backwards) actually gives us a linear combination of 113 and 355 yielding 1. In fact, isolating 16 from the second equation and putting into the first one gives

\[ 355 = 113 \cdot 3 + (113/7 - 1/7) \]

which reads 113 \cdot 22 - 355 \cdot 7 = 1 after clearing the denominators. So \( x_0 = 22 \) and \( y_0 = 7 \) is a solution of the given equation. Thus, the general solution is

\[ \{ x = 22 + 355n, \ y = 7 + 113n : n \in \mathbb{Z} \}. \]

2. (Davenport, p.217, ex.1.23*) We aim to show that the binomial coefficient \( \binom{p}{r} \) is divisible by \( p \) if \( p \) is prime and \( 1 \leq r < p \). First of all, the problem is well-posed because those quotients are indeed integers (for instance, being the coefficients of \( (1+x)^p \)). Observe that since \( r < p \) and \( p \) is prime, \( r! \) cannot be divisible by \( p \) (because \( (m, p) = 1 \) for \( m = 1, 2, \ldots, p-1 \)). So \( (r!, p) = 1 \). Similarly, \( ((p-r)!, p) = 1 \). This implies that \( (r!(p-r)!, p) = 1 \). Therefore, we conclude that \( p|\binom{p}{r} \).

3. (Davenport, pp.217, ex.1.24) We will show that there are infinitely many primes of the form \( 6k-1 \), \( k \in \mathbb{N} \). Assume, for a contradiction, that there are only finitely many of them, say \( p_1, p_2, \ldots, p_n \). Let \( N = 6(p_1 p_2 \ldots p_n) - 1 \). Since \( N \) is odd, it has an odd prime divisor, say \( p \). But an odd prime must be either of the form \( 6k + 1 \) or \( 6m - 1 \) (that is if one divides \( p \) by 6, the remainder cannot be 0, 2, 3, 4, by obvious reasons). Now, if \( p = 6n - 1 \), then it is one of the \( p_j \)'s \( (j = 1, 2, \ldots, n) \), and consequently it cannot divide \( N \). So, \( N \) must be the product of some primes of the form \( 6m + 1 \). On the other hand, observe that product of two numbers of the form \( 6m + 1 \) is also of the form \( 6m + 1 \). Thus, \( N = 6m + 1 \) for some \( m \). But this is impossible, since \( N \) is already of the form \( 6m - 1 \).

4. (Davenport, pp.217, ex. 2.01) Assume that \( a \equiv b \ mod \ kn \). We will show that \( a^k \equiv b^k \ mod \ k^2 n \). First, note the following fact: if \( c \equiv d \ mod \ mn \) then \( c \equiv d \ mod \ m \). This is because if \( mn \) divides \( c - d \), then obviously \( m \) divides \( c - d \), too. Now, we know that \( a^k - b^k = (a - b)(a^{k-1} + a^{k-2}b + \cdots + b^{k-1}) \). Then we have \( a^{k-1} + a^{k-2}b + \cdots + b^{k-1} \equiv a^{k-1} + a^{k-2}a + \cdots + a^{k-1} \equiv ka^{k-1} \ mod \ kn \) (replace \( b \) with \( a \) since they are congruent \( \mod \ kn \)). So, by our remark above \( a^{k-1} + a^{k-2}b + \cdots + b^{k-1} \equiv ka^{k-1} \equiv 0 \ mod \ k \). Since \( kn|(a-b) \) and \( k|a^{k-1} + a^{k-2}b + \cdots + b^{k-1} \), we deduce that \( k^2 n|a^k - b^k \), i.e. \( a^k \equiv b^k \ mod \ k^2 n \).

5. We claim that (34709, 100313) = 1. Indeed, by euclidean algorithm:

\[
\begin{align*}
100313 & = 34709 \cdot 2 + 30895 \\
34709 & = 30895 \cdot 1 + 3814 \\
30895 & = 38148 + 383 \\
3814 & = 383 \cdot 9 + 367 \\
383 & = 367 \cdot 1 + 16 \\
367 & = 16 \cdot 22 + 15 \\
16 & = 15 \cdot 1 + 1 \\
15 & = 1 \cdot 15.
\end{align*}
\]
Traversing the algorithm backwards, we get $1 = 16 \cdot 1 - 15 \cdot 1 = 16 \cdot 1 - (367 \cdot 1 - 16 \cdot 22) = 16 \cdot 23 - 367 \cdot 1 = \cdots = 100313 \cdot 2175 - 34709 \cdot 6286$.

6. It is clear that $(15, 35, 90) = 5$. To find a linear combination giving 5, we can again apply the euclidian algorithm for, say, 15 and 35, and get $5 = -2 \cdot 15 + 1 \cdot 35$. Finally, take the coefficient of 90 to be 0.

7. We will show that $(F_n, F_m) = F_{(m,n)}$. This will follow from the following well-known identity:

$$F_{m+n} = F_{m-1}F_n + F_m F_{n+1}, \quad \forall n, m \in \mathbb{N} \tag{1}$$

To prove this, fix $m \in \mathbb{N}$. We proceed by induction on $n$. For $n = 1$, right hand side (RHS) of the equation becomes $F_{m-1} F_1 + F_m F_2 = F_{m-1} + F_m$, which is equal to the left hand side (LHS), i.e. to $F_{m+1}$. When $n = 2$, the equation holds as well, because RHS $= F_{m-1} F_2 + F_m F_3 = F_{m-1} + 2F_m = (F_{m-1} + F_m) + F_m = F_{m+1} + F_m$, which is equal to the LHS, i.e. to $F_{m+2}$. Now, assume the equation holds for $k = 3, 4, \ldots, n$. We will show that it holds for $n+1$. Indeed,

for $k = n - 1$ we have $F_{m+n-1} = F_{m-1} F_{n-1} + F_m F_n$
for $k = n$ we have $F_{m+n} = F_{m-1} F_n + F_m F_{n+1}$.

Adding both sides of these equations will give:

$$\text{LHS} = F_{m+n-1} + F_{m+n} = F_{m+n+1}$$
$$\text{RHS} = F_{m-1} F_{n-1} + F_m F_n + F_{m-1} F_n + F_m F_{n+1}$$
$$= F_{m-1}(F_{n-1} + F_n) + F_m(F_n + F_{n+1})$$
$$= F_{m-1} F_{n+1} + F_m F_{n+2}$$

which is the equation for $k = n + 1$, as required. So we proved that the equation (1) holds. Alternatively, one could use the formula $F_n = (\sigma^n - \tau^n)/\sqrt{5}$ that we proved in HW1, and substitute it in (1) and check that both sides of the equation are indeed equal.

From this identity we can deduce that

$$(F_m, F_{n+m}) = (F_m, F_n) \tag{2}$$

To show this, first note that two consecutive Fibonacci numbers are coprime, i.e. $(F_n, F_{n+1}) = 1$ (apply euclidian algorithm for $F_{n+1}$ and $F_n$), and see that the last nonzero remainder is $F_1 = 1$. Now, $(F_m, F_{n+m}) = (F_m, F_{m-1} F_{n-1} + F_m F_n) = (F_m, F_{m-1} F_n) = (F_m, F_n)$. The last equality follows from the fact that $F_m$ and $F_{m-1}$ are coprime.

If we iterate identity (2) $a$ times, then we get $(F_m, F_n) = (F_m, F_{n+m}) = (F_m, F_{n+2m}) = \cdots = (F_m, F_{n+a m})$. In particular, if $n = m$, then we deduce that $(F_m, F_{(a+1)m}) = (F_m, F_m) = F_m$.

Putting this in other words: if $m|M$, then $F_m|F_M$.

Now, if we assume $n > m$ and apply euclidian algorithm, we get

$$n = a_1 m + r_1$$
$$m = a_2 r_1 + r_2$$
$$r_1 = a_3 r_2 + r_3$$
$$\ldots$$
$$r_k = a_{k+2} r_{k+1} + d$$

where $d = (n, m)$. Using the above remark, we obtain that $(F_n, F_m) = (F_{a_1 m + r_1}, F_m) = (F_{r_1}, F_m)$ from the first line. Similarly, $(F_{r_1}, F_m) = (F_{r_2}, F_m)$ from the second line. Finally, the last line tells $(F_{r_k}, F_{r_{k+1}}) = (F_{r_{k+1}}, F_d) = F_d$ (because $F_d|F_{r_{k+1}}$ since $d|r_{k+1}$). Combining all of these, we get $(F_n, F_m) = F_d$, as desired.

8. Let $n$ be a positive integer, and $p$ any prime. Let $\alpha$ be the largest power of $p$ dividing $n!$, that is, $p^\alpha | n!$ but $p^{\alpha+1} \nmid n!$ (in this case, we say that $p^\alpha$ exactly divides $n!$, and denote by
12. We want to find all solutions of the equation $x^11 = 101$, which gives $k = 9$, $z = 41$.

9. We will find the number of $N$ zeros at the end of $1000!$ in decimal notation. Clearly, $10^N||1000!$. But to get a factor of 10 we must have a 2 and a 5 in the prime factorization of $1000!$. So, if $2^a||1000!$ and $5^b||1000!$, then $N = \min\{a, b\}$. Clearly, $a > b$; so, in fact $N = b$. Now, $b$ can be found by the previous problem (with $p = 5$) as $b = |1000/5| + |1000/25| + |1000/125| + |1000/625| = 200 + 40 + 8 + 1 = 249$.

10. We will find the prime factorization of $2^{36} - 1$. This will follow from multiple applications of elementary identities: $2^{36} - 1 = (2^{18} - 1)(2^{18} + 1)$. $2^{18} - 1 = (2^9 - 1)(2^9 + 1)$. $2^9 - 1 = (2^3 - 1)(2^3 + 2^3 + 1) = 7 \cdot 73$. $2^9 + 1 = (2^3 + 1)((2^3)^2 - 3^3 + 1) = 3^3 \cdot 19$. Similarly $2^{18} + 1 = 5 \cdot 13 \cdot 37 \cdot 109$.

11. We would like to find $\min(x+y)$ among positive integer solutions $(x, y)$ of the equation $18x + 33y = 549$. By the euclidian algorithm, it is straightforward (yet cumbersome) to get $549 = 18 \cdot 36 + 13 \cdot 18 - 63$. So, solutions of this equation are of the form $(x, y) = (36 + 11k, -183 - 6k)$. The requirement that $x, y$ be positive, reduces to three possibilities for $k$, namely $k = -31, -32, -33$. So we get three solutions: $(25, 3)$, $(15, 9)$, $(3, 15)$. So the minimum of $x + y$ is attained by the last solution: $x = 3, y = 15, x + y = 18$.

12. We want to find all solutions of the equation $x+10y+25z = 99$ for $x, y, z$ nonnegative integers. First of all, note that $x$ must be of the form $99 - 5n$, because $10y + 25z = 99 - x$, i.e. $5n = 99 - x$ for some $n$. Then (equivalently) we would like to solve $10y + 25z = 5n$ (for $y$ and $z$). By the euclidian algorithm again, we obtain that $(10, 25) = 5 = 2 \cdot 10 + 1 \cdot 25$. So, $5n = -2n \cdot 10 + n \cdot 25$ is a solution of the above equation. The general solution is then of the form $(y, z) = (-2n + 5k, n - 2k)$. In other words, $x = 99 - 5n, y = -2n + 5k, z = n - 2k$ give a solution (provided they are nonnegative). So one should start plugging values for $n = 0, 1, 2, \ldots, 19$ and find all $k$’s such that $y$ and $z$ are positive. Although it is not very hard to do it by hand, a short computer program (for instance, written in pari) will save our time:

```
for(n=0,19,for(k=0,10,(if(sign(-2*n+5*k)+1,(if(sign(n-2*k)+1,print(99-5*n,-2*n+5*k,n-2*k))))))
```

The output is:

```
(99,0,0) (89,1,0) (79,2,0) (74,0,1) (69,3,0) (64,1,1) (59,4,0) (54,2,1) (49,0,2) (49,5,0) (44,3,1) (39,1,2) (39,6,0) (34,4,1) (29,2,2) (29,7,0) (24,0,3) (24,5,1) (19,3,2) (19,8,0) (14,1,3) (14,6,1) (9,4,2) (9,9,0) (4,2,3) (4,7,1)
```

13. This time we would like to solve $140x + 110y + 78z = 6548$ such that $x + y + z = 69$, and $x, y, z \geq 0$. Plugging $x = 69 - y - z$ in the first equation gives $30y + 62z = 3112$. Using the euclidian algorithm, we obtain a solution $(-3112, 1556)$. So, the general solution is $(y, z) = (-3112 + 31k, 1556 - 15k)$. So we should find the $k$ value for which $y, z$ and $x = 69 - y - z$ are all nonnegative. It is easy to see that the only $k$ value satisfying this is $k = 101$, which gives $x = 9, y = 19, z = 41$. 

```