Math 301 A - Spring 2014
Final Exam
June 11, 2014
Solutions

1. *Prove that the product of three consecutive integers is divisible by 60 if the middle integer is a perfect square.*

   Proof: Let n be a perfect square, and let $P = (n-1)n(n+1)$ be the product of the three consecutive integers with n in the middle.

   Since n is a perfect square, n is congruent to 0 or 1 modulo 4.

   If $n \equiv 0 \pmod 4$, then $4|P$.

   If $n \equiv 1 \pmod 4$, then $n-1 \equiv 0 \pmod 4$, and so $4|n-1$, and hence $4|P$.

   Thus, $4|P$.

   We have that n is congruent to 0, 1, or 2 modulo 3. If $n \equiv 0 \pmod 3$, then $3|n$ and $3|P$.

   If $n \equiv 1 \pmod 3$, then $3|n-1$, and $3|P$.

   If $n \equiv 2 \pmod 3$, then $3|n+1$, and $3|P$.

   Thus $3|P$.

   Looking at squares modulo 5, we see:

n	$n^2 \bmod 5$
0	0
1	1
2	4
3	4
4	1

   Hence, n is congruent to $0, 1$, or 4. For each value we have $n, n-1$, and $n+1$ congruent to 0 modulo 5, respectively.

   Hence, $5|P$.

   Since $3|P$, $4|P$ and $5|P$, and $(3,4,5) = 1$, we conclude that $3 \cdot 4 \cdot 5 = 60|P$. ■

2. *Let i be a non-negative integer. Prove that the number*

   $$8 \cdot 64^i + 25 \cdot 7^i$$

   is not prime.

   Proof: We can start by observing that

   $$8 \cdot 64^0 + 25 \cdot 7^0 = 33 \equiv 0 \pmod 3$$
   $$8 \cdot 64^1 + 25 \cdot 7^1 = 687 \equiv 0 \pmod 3$$
   $$8 \cdot 64^2 + 25 \cdot 7^2 = 33993 \equiv 0 \pmod 3$$

and this gives us the idea that perhaps $8 \cdot 64^i + 25 \cdot 7^i$ is always divisible by 3.

Reducing modulo 3, we find that $8 \cdot 64^i + 25 \cdot 7^i \equiv 2 \cdot 1^i + 1 \cdot 1^i \equiv 3 \equiv 0 \pmod 3$.

Hence, 3 always divides $8 \cdot 64^i + 25 \cdot 7^i$ for non-negative i.

Since $8 \cdot 64^i + 25 \cdot 7^i \geq 8 \cdot 64^0 + 25 \cdot 7^0 = 33 > 3$, we conclude that $8 \cdot 64^i + 25 \cdot 7^i$ is never prime for non-negative i. ■

3. *Suppose x is the smallest integer greater than 10000 such that*

$$3x \equiv 5 \pmod{61} \text{ and } 5x \equiv 3 \pmod{62}.$$

Find x.

Multiplying $3x \equiv 5 \pmod{61}$ by 20 yields $60x \equiv 100 \pmod{61}$ and subtracting this from $61x \equiv 61 \pmod{61}$ yields

$$x \equiv -39 \equiv 22 \pmod{61}.$$

Thus $x = 22 + 61k$ for some integer k.

Using the second given congruence yields

$$\begin{aligned} 5(22 + 61k) &\equiv 3 \pmod{62} \\ 110 + 305k &\equiv 3 \pmod{62} \\ 57k &\equiv 17 \pmod{62} \end{aligned}$$

Sutracting this last congruence from $62k \equiv 62 \pmod{62}$ yields

$$5k \equiv 45 \pmod{62}$$

and since 5 divides 45, and $(45, 62) = 1$, we conclude

$$k \equiv 9 \pmod{62}.$$

Thus $k = 9 + 62m$ for some integer m, and hence $x = 22 + 61(9 + 62m) = 571 + 3782m$.

Since $2 < 10000/3782 < 3$, and $8135 = 571 + 3782 \cdot 2$ and $11917 = 571 + 3782 \cdot 3$, we conclude that $x = 11917$.

4. *Find the largest integer that cannot be expressed as a sum of non-negative multiples of 5, 7 and 13. Prove that this is the largest such integer.*

16 is the largest such integer.

First we prove that 16 cannot be expressed as a sum of non-negative multiples of 5, 7, and 13.

Suppose $16 = 5a + 7b + 13c$ where a, b and c are non-negative integers.

Since $2 \cdot 13 = 26 > 16$, we conclude that $c = 0$ or $c = 1$.

Suppose $c = 1$. Then $3 = 5a + 7b$, but $5a + 7b >= 5$ unless $a = b = 0$, in which case $3 = 0$, a contradiction. So $c \neq 1$.

Suppose $c = 0$. Then $16 = 5a + 7b$. Since $7 \cdot 3 = 21 > 16$, $b = 0, 1$, or 2. If $b = 0$, then $a = 16/5$ which is not an integer. If $b = 1$, then $a = 9/5$ which is not an integer. If $b = 2$, then $a = 2/5$ which is not an integer. In all three cases, we have a contradiction. So $c \neq 0$.

Thus we arrive at the contradiction that $c = 0$ or $c = 1$ and $c \neq 0$ and $c \neq 1$.

Hence our assumption that 16 was so expressible was false, and we conclude that 16 is not so expressible.

Now,

$$\begin{aligned} 17 &= 5 \cdot 2 + 7 \cdot 1 + 13 \cdot 0 \\ 18 &= 5 \cdot 1 + 7 \cdot 0 + 13 \cdot 1 \\ 19 &= 5 \cdot 1 + 7 \cdot 2 + 13 \cdot 0 \\ 20 &= 5 \cdot 4 + 7 \cdot 0 + 13 \cdot 0 \\ \text{and } 21 &= 5 \cdot 0 + 7 \cdot 3 + 13 \cdot 0. \end{aligned}$$

Let $m > 21$ be an integer. Then m is congruent to one of $17, 18, 19, 20$, or 21 modulo 5. Say m is congruent to z modulo 5, and $17 \leq z \leq 21$ and $z = 5r + 7s + 13t$. Then $m = 5r + 7s + 13t + 5u = 5(r + u) + 7s + 13t$ for some positive integer u, and so every integer greater than 16 can be represented as the sum of non-negative multiples of 5, 7, and 13.

5. *Suppose (x, y, z) is a primitive Pythagorean triple, with $z > x$ and $z > y$. Prove that 3 divides exactly one of x and y, and 3 does not divide z. (If you wish to use a result proved in homework, you will need to prove it again here.)*

   Proof: We could prove this using our theorem on primitive pythagorean triples, but here I'll give a proof that doesn't use this.

   Suppose (x, y, z) is a primitive pythagorean triple, with $z > x$ and $z > y$.

   Then $x^2 + y^2 = z^2$, and the gcd of x,y, and z is 1.

   As a result, we know that 3 does not divide all three values, x, y, and z.

   The squares modulo 3 are 0 and 1.

   Note that, for any integer n, $3|n$ iff $3|n^2$.

   Adding these, we have the following table of possibilities:

+	0	1
0	0	1
1	1	2

   This tells us several things. First, that, since z^2 is the sum of two squares, it is not congruent to 2 mod 3, and hence x or y is congruent to 0 mod 3. However, x and y cannot *both* be congruent to 0 mod 3; for in that case, z would also be congruent to 0, and the triple would not be primitive. Hence, exactly one of x and y is divisible by 3, and as a result z is not divisible by 3. ■

6. *Prove that there are no solutions to $5x^2 + 7y^2 = z^2$ with $x, y, z \in \mathbb{Z}$ and $xyz \neq 0$.*

   Proof: Suppose $5x^2 + 7y^2 = z^2$ for some $x, y, z \in \mathbb{Z}$, and $xyz \neq 0$, with z as small as possible (i.e., suppose that if $5a^2 + 7b^2 = c^2$ with $a, b, c \in \mathbb{Z}$ and $abc \neq 0$, then $c \geq z$).

   We may assume without loss of generality that $x > 0$, $y > 0$ and $z > 0$. (For, if any of x, y and z is negative, we can replace it by its absolute value.)

Then $7y^2 \equiv z^2 \pmod 5$, i.e.

$$2y^2 \equiv z^2 \pmod 5.$$

In problem 1, we noted that the squares modulo 5 are 0, 1, and 4. Hence that possible values of $2y^2$ modulo 5 are 0, 2, and 3.

But, since $2y^2 \equiv z^2 \pmod 5$, $2y^2 \equiv z^2 \equiv 0 \pmod 5$.

Hence, $5|y^2$, and so $5|y$. Also, $5|z^2$, and $5|z$.

Write $y = 5y'$ and $z = 5z'$ for some integers y' and z'.

Then

$$\begin{aligned} 5x^2 + 7(5y')^2 &= (5z')^2 \\ 5x^2 + 25 \cdot 7y'^2 &= 25z'^2 \\ x^2 + 5 \cdot 7y'^2 &= 5z'^2 \end{aligned}$$

and so $5|x^2$ and $5|x$.

Write $x = 5x'$ for some integer x'.

Then

$$5(5x')^2 + 7(5y')^2 = (5z')^2$$

so

$$5(x')^2 + 7(y')^2 = (z')^2.$$

However, since $z > 0$, $z' < z$, and this is a contradiction to our assumption that we had the solution with the smallest possible z.

Hence, there is no solution to $5x^2 + 7y^2 = z^2$, with $x, y, z \in \mathbb{Z}$, and $xyz \neq 0$. ■

7. *Define the sequence $\{a_n\}$ by*

$$a_0 = 1, a_1 = 1, \text{ and } a_n = a_{n-1} - a_{n-2} \text{ for } n \geq 2.$$

Express the generating function for $\{a_n\}$ as a rational function (i.e., not as a series).

Let $A(x) = \sum_{n=0}^{\infty} a_n x^n$.

From $a_n = a_{n-1} - a_{n-2}$ for $n \geq 2$, we have

$$\begin{aligned} \sum_{n=2}^{\infty} &= \sum_{n=2}^{\infty} a_{n-1}x^n - \sum_{n=2}^{\infty} a_{n-2}x^n \\ &= \sum_{n=1}^{\infty} a_n x^{n+1} - \sum_{n=0}^{\infty} a_n x^{n+2} \\ A(x) - x - 1 &= x(A(x) - 1) - x^2(A(x)) \\ A(x) - xA(x) + x^2A(x) &= -x + x + 1 \\ A(x) &= \frac{1}{1 - x + x^2}. \end{aligned}$$