M328K – Rusin – HW3 ANSWERS – Due Thursday, Feb 9 2017

1. Prove that if $P(x) = a + bx + cx^2$ is a quadratic polynomial with integer coefficients $a, b, c$ and $n$ is an integer, then

$$r \equiv s \pmod{n} \quad \text{implies} \quad P(r) \equiv P(s) \pmod{n} .$$

Bonus: prove that the same is true for every integer polynomial $P$.

**ANSWER:** Using the fact that "congruences add and multiply" we conclude that if $r \equiv s$ then $r \cdot r \equiv s \equiv s$ (i.e. $r^2 \equiv s^2$), and then $c \cdot r^2 \equiv c \cdot s^2$. Similarly, $b \cdot r \equiv b \cdot s$. Adding these congruences (and the congruence that $a \equiv a$) we deduce that $P(r) \equiv P(s)$.

In the same way we prove that $P(r) \equiv P(s)$ for *any* integer polynomial $P(x)$; first use induction to prove that $r^n \equiv s^n$. You can also prove this by noting that, as polynomials in two variables, $P(x) - P(y)$ is a multiple of $(x - y)$; substitute in $x = r$ and $y = s$.

I would say the hardest thing about this problem is finding something to say beyond "this is pretty obvious"...

2. Show that for every integer $a$ not divisible by 11 there is another integer $b$ with $a \cdot b \equiv 1 \pmod{11}$ . Show also that this $b$ is unique modulo 11, that is, show that if $c$ is another integer with $a \cdot c \equiv 1 \pmod{11}$ then $b \equiv c \pmod{11}$ . (Hint: Bezout's Lemma is better than a case-by-case computation.)

**ANSWER:** If $a$ is not a multiple of 11, then since 11 is prime, $a$ has no common divisors with 11, i.e. gcd($a$,11)=1. But then Bezout's Lemma assures us that there are integers $b$ and $c$ with $ab + 11c = 1$, and in particular $ab \equiv 1 \pmod{11}$ . As for uniqueness, note that if $ab \equiv 1$ and $ac \equiv 1$ then $b \equiv 1 \cdot b \equiv cab \equiv c \cdot 1 \equiv c$.

As you can see from the proof, exactly the same statement can be made with 11 replaced with any other prime. If 11 is replaced by a composite number $n$ then the same conclusion applies if $a$ has no common divisor with $n$. In particular, each of the $\phi(n)$ integers between 1 and $n$ which is coprime to $n$ has an inverse (and we may take that inverse also to be one of these $\phi(n)$ integers). Here are the inverses modulo 11:

| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|
| 1 | 6 | 4 | 3 | 9 | 2 | 8 | 7 | 5 | 10 |

Here are the inverses modulo 12:

| 1 | 5 | 7 | 11 |
|---|---|---|---|
| 1 | 5 | 7 | 11 |

(That's right: every invertible element is its own inverse modulo 12!)

3. (a) Find a solution in integers $x, y$ to the equation $13x + 21y = 4$.

(b) Find another solution.

(c) Find another.

(d) Stop me from continuing this question *ad infinitum* by describing all the solution pairs $(x, y)$. (Hint: finding one solution is the hard part and you already did that; then

if $(x', y')$ were another solution, you'd have two equations to play with, one with $x, y$ and one with $x', y'$. Subtract, rearrange terms, and see what you can conclude...)

**ANSWER:** You are welcome to find solutions any way you like for parts (a),(b),(c). I went straight to (d) and found all solutions by examining the proof that solutions exist. That uses the Euclidean Algorithm, which as you know is an iteration of the Division Algorithm. So consider these Division Algorithm computations:

$$\begin{aligned} 21 &= 13 \cdot 1 + 8 \\ 13 &= 8 \cdot 1 + 5 \\ 8 &= 5 \cdot 1 + 3 \\ 5 &= 3 \cdot 1 + 2 \\ 3 &= 2 \cdot 1 + 1 \end{aligned}$$

at which point we quit because the last remainder (1) even divides the last divisor (2) with no remainder. Now turn these equations around:

$$\begin{aligned} 8 &= 1 \cdot 21 - 1 \cdot 13 \\ 5 &= 1 \cdot 13 - 1 \cdot 8 \\ 3 &= 1 \cdot 8 - 1 \cdot 5 \\ 2 &= 1 \cdot 5 - 1 \cdot 3 \\ 1 &= 1 \cdot 3 - 1 \cdot 2 \end{aligned}$$

Now substitute these into each other. You can work from the top down (to show that all kinds of things are linear combinations of 13 and 21) or from the bottom up (to show that 1 is a linear combination of many pairs of integers). For example, I see $5 = 1 \cdot 13 - 1 \cdot (1 \cdot 21 - 1 \cdot 13) = 2 \cdot 13 - 1 \cdot 21$ and then $3 = 2 \cdot 21 - 3 \cdot 13$, then $2 = 5 \cdot 13 - 3 \cdot 21$, and finally $1 = 5 \cdot 21 - 8 \cdot 13$.

There are ways to make the calculation more systematic, keeping track of various numbers while carrying out the Euclidean algorithm in the first place. You are welcome to perfect that skill – it's useful, as illustrated by problem 2 – but I don't want to go overboard this semester with computational algorithms.

Now, as for the complete set of solutions, note that if we have two pairs of solutions, i.e. if $13x + 21y = 4$ and $13x' + 21y' = 4$, then $13(x - x') + 21(y - y') = 0$, that is, $13(x - x') = 21(y' - y)$. Since 13 is prime and divides the product $21(y - y')$, it would have to divide one of those two factors. It doesn't divide 21, so it must divide $y' - y$, say, $y' - y = 13k$. Substitute and divide by 13 to conclude $x - x' = 21k$. Therefore, the second solution, $(x'y')$, is equal to the first solution $(x, y)$, plus an integer multiple of $(21, -13)$. Conversely, you can check that once one solution $(x, y)$ is found, every pair $(x', y') = (x + 21k, y - 13k)$ is also a solution.

More generally, if $\gcd(a, b)=1$, then all solutions $(x', y')$ to the equation $ax + by = 1$ can be obtained from one solution $(x, y)$ simply by adding multiples of $(b, -a)$. (I will let you figure out how to adjust this observation to cover the case that $d = \gcd(a, b) > 1$.)

4. Show that any two consecutive Fibonacci numbers are coprime. That is, for every $n \geq 0$, $\gcd(F_n, F_{n+1})$=1, where

$$F_0 = 1, \qquad F_1 = 1, \qquad \text{and} \qquad F_{n+1} = F_n + F_{n-1} \qquad \text{for } n \geq 1$$

**ANSWER:** This is a very typical proof by induction. The claim is that the sentence

$$P(n) = \text{“}F_n \text{ and } F_{n+1} \text{ are coprime”}$$

is true for all integers $n = 1, 2, 3, \ldots$. It's obviously true when $n = 0$ and $n = 1$, for example.

Now, if $P(n)$ is true for all $n < N$, say, then let us also show it's true when $n = N$. Let $d = \gcd(F_N, F_{N+1})$. Then in particular $d$ divides both $F_N$ and $F_{N+1}$, and hence their difference $F_{N+1} - F_N = F_{N-1}$ as well. Yet by induction $F_N$ and $F_{N-1}$ have no common factors ($> 1$); thus $d = 1$. This completes the induction step, and hence the proof of the claim.

To a number theorist, the Fibonacci numbers are a treaure trove of interesting theorems and conjectures. For example, one may show that $F_n$ divides $F_m$ precisely when $n + 1$ divides $m + 1$ !

5. Compute the gcd of $A = 273413, B = 57575$

**ANSWER:** THe gcd is 7. I expected you to use the Euclidean Algorithm: the successive remainder are 43113, 14462, 14189, 273, 266, and 7.

I did NOT expect you to factor these integers but the prime factorizations are $7 \cdot 139 \cdot 281$ and $5^2 \cdot 7^2 \cdot 47$ respectively, so that the gcd is clearly 7.

Challenge question: Ten islanders have a large pile of coconuts that they wish to share equally. One by one they count off the coconuts, to make sure all the piles are even, but at the end only nine coconuts remain in the last round; they would have nine coconuts left after dividing them as evenly as possible. So one member of the tribe is voted off the island and the remaining nine people start all over again to divide the coconuts. Unfortunately, by the end they discover they have 8 leftover coconuts, and cannot distribute those evenly amongst themselves. You can imagine how this goes: every time they vote someone off the island, the remaining members find they cannot evenly share the pile of coconuts because in the last round they have one coconut too few to share evenly. The problem is finally solved when the last two islanders find one leftover coconut, and one of those two throws the other one into the sea, keeping all the cocounts to himself, thus making the island Great Again.

How many coconuts were there in the first place?

**ANSWER:** The possible answers are those of the form $2520n-1$ ($n = 1, 2, 3, \ldots$). Without any instructions to the contrary I suppose 2519 would be “the” right answer.

The point is that the number $N$ of coconuts is to be an integer which is congruent to 9 modulo 10, congruent to 8 modulo 9, ..., and congruent to 1 modulo 2. I wanted you to wrestle with this question to anticipate the Chinese Remainder Theorem, which can be

used to prove that there are solutions (and to compute them all). But in this particular problem it's not as hard as it looks to find all solutions: the integer $-1$ satisfies all these congruences, so we may equivalently state the problem as: we need to find a (positive) integer $N$ which satisfies

$$N \equiv -1 \pmod{10}\ , \qquad N \equiv -1 \pmod{9}\ , \quad \ldots \quad N \equiv -1 \pmod{2}$$

Stated in more primitive language, what we need is for $N+1$ to be a multiple of 10, of 9, ..., of 2. That is, we need $N+1$ to be a common multiple of the first 10 positive integers. If you think of what the prime factors of $N+1$ must be to accomplish this, you see it is necessary and sufficient that $N+1$ be a multiple of $2^3 3^2 5^1 7^1 = 2520$.