Math 4150-B, Intro to Number Theory
EXAM 1
February 13, 2018

Solutions

1. Let $F_0, F_1, F_2, \ldots$ be the Fibonacci numbers, given by $F_0 = F_1 = 1$ and $F_{n+1} = F_n + F_{n-1}$ for each $n \geq 1$. Prove that the gcd of two consecutive Fibonacci numbers is always 1.

   Solution:

   Suppose that two consecutive Fibonacci numbers shared a common factor larger than 1. That is, suppose that $p|F_n$, F_{n+1} for some n and for some prime p. Then by the definition of Fibonacci numbers, p divides $F_{n+1} - F_n = F_{n-1}$. Similarly, since p divides both F_n and F_{n-1}, p divides the difference, F_{n-2}. Continuing in this way, we find that p_{F_1} and F_0, namely, $p|(1, 1)$. But this is a contradiction, as $p|1$ implies $p = \pm 1$, but p was a prime.

2. If a and b are relatively prime natural numbers, find, with proof, the greatest common divisor $(a^2 + b^2, a + b)$. and prove your answer.

   Solution:

   Suppose that a prime p divides both $a + b$ and $a^2 + b^2$. As $p|(a + b)$, we have $a \equiv -b \pmod{p}$. Thus, $a^2 + b^2 \equiv 2b^2 \equiv 0 \pmod{p}$. There are two cases. First, suppose that p is odd. In this case, we have that $p|b^2$, and so $p|b$. But then $a \equiv -0 \equiv 0 \pmod{p}$. This contradicts the assumption that a and b are relatively prime. Thus, no odd prime can divide the gcd of these two numbers. Now we consider the case when $p = 2$. We have shown that the gcd in question is always 1 or 2, and need to distinguish between these cases. Now2 divides both $a^2 + b^2$ and $a + b$ if and only if both of these numbers are even. This occurs if and only if the parity of a and b are equal. Since a and b are relatively prime, they cannot both be even, so this happens if and only if a and b are both odd. Furthermore, if a and b are both odd, then a^2 and b^2 are too, so the gcd of the two numbers really is odd. Thus, $(a^2 + b^2, a + b) = \frac{1}{2}\left(3 + (-1)^{a+b}\right)$ (this is just a slightly more convenient way of writing this piecewise function, and expressing it via its values in 2 cases is also ok).

3. (a) Compute $\varphi(1000)$.

   (b) Use Euler's theorem to find the last three digits of 13^{5602}.

   Solution:

   Using the multiplicivity of φ and the formula $\varphi(p^n) = p^n - p^{n-1}$ for its values on prime powers, we compute $\varphi(1000) = \varphi(2^3)\varphi(5^3) = (2^3 - 2^2)(5^3 - 5^2) = (8 - 4)(125 - 25) = 4 \cdot 100 = 400$. Thus, if $(a, 1000) = 1$, i.e., if a is odd and not divisible by 5, Euler's theorem tells us that $a^{400} \equiv 1 \pmod{1000}$. Thus, since 13 satisfies this condition, we have $13^{5602} \equiv 13^{5600} \cdot 13^2 \equiv 13^{400 \cdot 14} \cdot 169 \equiv 1 \cdot 169 \equiv 169 \pmod{1000}$. Thus, the last three digits in question are 169.

4. Find all integers x which satisfy the following system of linear congruences:

$$\begin{aligned} x &\equiv 3 \pmod 5, \\ x &\equiv 7 \pmod 8, \\ x &\equiv 5 \pmod 7. \end{aligned}$$

Solution:

We will apply the Chinese Remainder Theorem. This is applicable as all three moduli are pairwise coprime. In the notation of the proof we gave in class, we have $M_1 = 56$, $M_2 = 35$, and $M_3 = 40$. We now look for inverses y_j of each M_j modulo m_j. For $j = 1$, we want the inverse of 56 modulo 5. We first reduce 56 mod 5 to get 1, which is clearly its own inverse, $y_1 = 1$. We next want an inverse of 35 modulo 8. Reducing, we obtain $3y_2 \equiv 1 \pmod 8$, so we can take $y_2 = 3$. Finally, for $j = 3$, we want to find an inverse of 40 modulo 7. That is, we want an inverse of 5 mod 7. The reduced representative mod 7 is quickly found to be 3 (by guess-and-check, for example). Thus, we can take $y_3 = 3$. Thus, our solution is $x = 3 \cdot 56 \cdot 1 + 7 \cdot 35 \cdot 3 + 5 \cdot 40 \cdot 3 = 168 + 735 + 600 \equiv 168 + 175 + 40 \equiv 383 \equiv 103 \pmod{280}$. This means that all integers x satisfying the system are those integers satisfying $x \equiv 103 \pmod{280}$.

5. Use the general theorem from class on the set of solutions (i.e., brute force guessing isn't allowed, and in each part you must state which case of the general theorem applies/what it says) to linear congruences to solve the following equations:

   (a) $2x \equiv 6 \pmod{10}$.

   (b) $5x \equiv 7 \pmod{10}$.

   (c) $3x \equiv 7 \pmod{10}$.

   Solution: We know that the equation $ax \equiv b \pmod m$ has no solutions if $d = (a, m) \nmid b$, and has d distinct solutions mod m otherwise.

   In (a), we have $(2, 10) = 2|6$, and so there are two different solutions modulo 10. To find them, we first find a particular solution. For this, we want to solve the linear diophantine equation $2x + 10y = 6$(it doesn't matter if we call the second factor $10y$ or $-10y$). There is a common factor of 2 in all terms, so we can reduce to the equation $x + 5y = 3$. Since the coefficients of x and y, 1 and -5, are relatively prime, we can find the linear combination we want by finding a linear combination of 1 and 5 which gives 1, and then we can multiply the whole equation by 3. This is easy in this case; we have simply $1 \cdot 1 + 0 \cdot 5 = 1$. Multiplying by 3 gives us $3 \cdot 1 + 0 \cdot 5 = 3$. Thus, a particular solution to the above equation is $x = 3$. This equation is really an equation modulo 5, as seen by the above argument where we divided out by 2's, and so the solutions modulo 10 are the two congruence classes lying "above" the class of 3 mod 5, namely $x \equiv 3, 8 \pmod{10}$. This is also exactly what the formula from the proof of our main theorem on linear congruences says.

   For (b), we find that $(5, 10) = 5 \nmid 7$, so there are no solutions.

For (c), we have $(3, 10) = 1$, and so there is a unique solution modulo 10. To find this, we can find an inverse of 3 mod 10, and then we would have $x \equiv \overline{3} \cdot 7 \pmod{10}$ as our solution. To find the inverse of 3 mod 10, we perform the Euclidean Algorithm, yielding $10 = 3 \cdot 3 + 1$, $3 = 3 \cdot 1 = 0$, and so $10 - 3 \cdot 3 = 1$. Reducing this equation mod 10 shows that $\overline{3} \equiv -3 \equiv 7 \pmod{10}$. Now $\overline{3} \cdot 7 \equiv -3 \cdot 7 \equiv -21 \equiv -1 \pmod{10}$. Thus, the solutions to (c) are $x \equiv -1 \pmod{10}$ (or 9 mod 10 if you prefer the reduced representative between 0 and 9).