

Solutions to Homework Assignment 6

Math 74, Fall 2006

December 2, 2006

1.

Theorem 1. *Let F_n denote the n th Fibonacci number. Then*

$$\gcd(F_{n+1}, F_n) = 1$$

for every $n \in \mathbb{N}^*$.

Proof. We will proceed by induction on n . Recall that the Fibonacci numbers are defined recursively by

$$\begin{aligned} F_1 &= F_2 = 1 \\ F_{n+2} &= F_n + F_{n+1} \quad (n \geq 2). \end{aligned}$$

Obviously

$$\gcd(F_2, F_1) = \gcd(1, 1) = 1.$$

Now suppose that $\gcd(F_k, F_{k+1}) = 1$ for some positive integer k . Using Lemma 4.40 in the lecture notes, we see that

$$\gcd(F_{k+2}, F_{k+1}) = \gcd(F_{k+1}, F_{k+2} \bmod F_{k+1}).$$

The proof will now be complete once we show that $F_{k+2} \bmod F_{k+1} = F_k$. But this follows immediately from the Division Algorithm, since

$$F_{k+2} = F_{k+1} + F_k \quad \text{and} \quad 0 \leq F_k < F_{k+1}.$$

□

2. In the proof of the Euclidean Algorithm of page 53-54 of the lecture notes, we proved that

$$\{1602x + 1170y \mid x, y \in \mathbb{Z}\} = \{k \gcd(1602, 1170) \mid k \in \mathbb{Z}\}.$$

So we may rephrase our problem as: what is the smallest positive integer b such that $10^6 + b$ is a multiple of $\gcd(1602, 1170)$. To answer this question, we first carry out the Euclidean Algorithm to calculate $\gcd(1602, 1170)$:

$$\begin{aligned} \gcd(1602, 1170) &= \gcd(1170, 432) \quad (432 = 1602 \bmod 1170) \\ &= \gcd(432, 306) \quad (306 = 1170 \bmod 432) \\ &= \gcd(306, 126) \quad (126 = 432 \bmod 306) \\ &= \gcd(126, 54) \quad (54 = 306 \bmod 126) \\ &= \gcd(54, 18) \quad (18 = 126 \bmod 54) \\ &= 18. \end{aligned}$$

By performing the Euclidean Algorithm more carefully (or performing back substitution), one may check that

$$(1) \quad 19 \cdot 1602 + (-26) \cdot 1170 = 18.$$

Therefore, our problem is equivalent to searching for the smallest positive integer b for which $10^6 + b$ is divisible by 18. We will now calculate $10^6 \bmod 18$:

$$\begin{aligned} 10^1 &\equiv 10 \pmod{18}, \\ 10^2 &\equiv 10 \pmod{18}, \\ 10^4 &\equiv 10 \pmod{18}, \end{aligned}$$

so we see that $10^6 = 10^4 \cdot 10^2 \equiv 10 \cdot 10 \equiv 10 \pmod{18}$. Therefore, the smallest integer b for which $10^6 + b$ is divisible by 18 is $b = 8$. To find an explicit x and y solving the equation

$$1602x + 1170y = 10^6 + 8,$$

we divide 1000008 by 18 to get $18 \cdot 55556 = 1000008$. Now multiply equation (1) by 55556 to get

$$1000008 = 55556 \cdot 18 = 55556 \cdot (19 \cdot 1602 + (-26) \cdot 1170) = 1602x + 1170y$$

where $x = 19 \cdot 55556 = 1055564$ and $y = -26 \cdot 55556 = 1444456$.

3. (a) Notice that

$$2^1 \equiv 2 \not\equiv 1 \equiv 16 \equiv 2^4 \pmod{3}$$

even though $1 \equiv 4 \pmod{3}$.

(b) We will show that $2^{70} + 3^{70}$ is divisible by 13. First, we calculate

$$\begin{aligned} 2^1 &\equiv 2 \pmod{13}, \\ 2^2 &\equiv 4 \pmod{13}, \\ 2^4 &\equiv 3 \pmod{13}, \\ 2^8 &\equiv 3 \cdot 3 \equiv 9 \pmod{13}, \\ 2^{16} &\equiv 9 \cdot 9 \equiv 81 \equiv 3 \pmod{13}, \\ 2^{32} &\equiv 3 \cdot 3 \equiv 9 \pmod{13}, \\ 2^{64} &\equiv 9 \cdot 9 \equiv 3 \pmod{13}, \end{aligned}$$

and so we get that

$$2^{70} \equiv 2^6 4 \cdot 2^4 \cdot 2^2 \equiv 3 \cdot 3 \cdot 4 \equiv 5 \pmod{13}.$$

Similarly, we calculate

$$\begin{aligned} 3^1 &\equiv 3 \pmod{13}, \\ 3^2 &\equiv 9 \pmod{13}, \\ 3^4 &\equiv 9 \cdot 9 \equiv 3 \pmod{13}, \\ 3^8 &\equiv 3 \cdot 3 \equiv 9 \pmod{13}, \\ 3^{16} &\equiv 9 \cdot 9 \equiv 3 \pmod{13}, \\ 3^{32} &\equiv 3 \cdot 3 \equiv 9 \pmod{13}, \\ 3^{64} &\equiv 9 \cdot 9 \equiv 3 \pmod{13}, \end{aligned}$$

and thus

$$3^{70} \equiv 3^{64} \cdot 3^4 \cdot 3^2 \equiv 3 \cdot 3 \cdot 9 \equiv 3 \pmod{13}.$$

Therefore,

$$2^{70} + 3^{70} \equiv 10 + 3 \equiv 0 \pmod{13}.$$

(c) We will now calculate the last two digits of 3^{1200} .

$$\begin{aligned} 3^1 &\equiv 3 \pmod{100}, \\ 3^2 &\equiv 9 \pmod{100}, \\ 3^4 &\equiv 81 \pmod{100}, \\ 3^8 &\equiv 81 \cdot 81 \equiv 61 \pmod{100}, \\ 3^{16} &\equiv 61 \cdot 61 \equiv 21 \pmod{100}, \\ 3^{32} &\equiv 21 \cdot 21 \equiv 41 \pmod{100}, \\ 3^{64} &\equiv 41 \cdot 41 \equiv 81 \pmod{100}, \\ 3^{128} &\equiv 81 \cdot 81 \equiv 61 \pmod{100}, \\ 3^{256} &\equiv 61 \cdot 61 \equiv 21 \pmod{100}, \\ 3^{512} &\equiv 21 \cdot 21 \equiv 41 \pmod{100}, \\ 3^{1024} &\equiv 41 \cdot 41 \equiv 81 \pmod{100}, \end{aligned}$$

and thus

$$\begin{aligned} 3^{1200} &\equiv 3^{1024} \cdot 3^{128} \cdot 3^{32} \cdot 3^{16} \\ &\equiv 81 \cdot 61 \cdot 41 \cdot 21 \\ &\equiv 41 \cdot 41 \cdot 21 \\ &\equiv 81 \cdot 21 \\ &\equiv 61 \pmod{100}. \end{aligned}$$

Thus the last two digits of the integer 3^{1200} are 6 and 1.

4.

Proposition 2. *Suppose that $n > 1$ is an integer such that $2^n + n^2$ is prime. Then n is divisible by 3.*

Proof. We will break the proof into multiple steps.

Step 1. *If $p > 3$ is a prime, then $p \equiv 1 \pmod{6}$ or $p \equiv 5 \pmod{6}$.*

If p is a prime greater than 3, then p is not divisible by 2 or 3. An integer which is congruent to either 0, 2, 3, or 4 modulo 6 is divisible by 2 or 3. Hence p is not congruent to 0, 2, 3, or 4 modulo 6. It follows that p is congruent to either 1 or 5 modulo 6.

Step 2. *If $n > 1$ such that $n^2 + 2^n$ is prime, then n is odd.*

If $n > 1$, then clearly $n^2 + 2^n > 3$. Therefore, if $n^2 + 2^n$ is prime, it cannot be divisible by 2. But if n is even, then $n^2 + 2^n$ is divisible by 2. Therefore, we see that if $n > 1$ and $n^2 + 2^n$ is prime, then n must be odd.

Step 3. *If $n > 1$ is odd, then $2^n \equiv 2 \pmod{6}$.*

We prove this step by induction. Clearly $2^1 \equiv 2 \pmod{6}$. So suppose that $k \geq 0$ is an integer for which $2^{2k+1} \equiv 2 \pmod{6}$. Then

$$2^{2(k+1)+1} \equiv 2^{2k+3} 4 \cdot 2^{2k+1} \equiv 4 \cdot 2 \equiv 8 \equiv 2 \pmod{6}.$$

Thus it follows by induction that $2^{2m+1} \equiv 2 \pmod{6}$ for all $m \geq 0$.

Step 4. Completion of the proof

We will now complete the proof. Suppose that $n > 1$ such that $n^2 + 2^n$ is prime. Since $n^2 + 2^n > 3$, by Step 1 either

$$n^2 + 2^n \equiv 1 \pmod{6}$$

or

$$n^2 + 2^n \equiv 5 \pmod{6}.$$

By Step 2, we see that n is odd. By Step 3, we see that $2^n \equiv 2 \pmod{6}$. Therefore, subtracting 2 from the congruences above, we see that either $n^2 \equiv 5 \pmod{6}$ or $n^2 \equiv 3 \pmod{6}$. Since $1^2 \equiv 5^2 \equiv 1 \pmod{6}$, we see that n is neither congruent to 1 nor 5 modulo 6. Since n is odd, it must be congruent to 3 modulo 6. This implies that n is a multiple of 3. \square