Math 400 — Examination No. 2
Due: Friday, May 11th, by 4:00PM

Dana Merrick
June 14, 2010

(1) *Fibonacci Numbers*

Recall that the sequence of Fibonacci numbers $\{F_i\}_{i=0}^{\infty}$ is defined recursively as follows:

$$F_1 = F_2 = 1$$

$$F_n = F_{n-1} + F_{n-2},\ n \geq 3.$$

(a) (i) Prove that for $n \geq 1$, F_n and F_{n+1} are *relatively prime*, that is

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

Recall that for a, $b \in \mathbb{Z}$, not both zero, $\gcd(a, b) = 1$ if and only if there exist s, $t \in \mathbb{Z}$ such that $1 = sa + tb$.

Proof. We will use the Euclidean algorithm to find $\gcd(F_n, F_{n+1})$. We have:

$$\begin{aligned} F_{n+1} &= 1 \cdot F_n + F_{n-1} \\ F_n &= 1 \cdot F_{n-1} + F_{n-2} \\ &\vdots \\ F_4 &= 1 \cdot F_3 + F_2 \\ F_3 &= 2 \cdot F_2 + 0 \end{aligned}$$

Substituting in $F_4 = 3$, $F_3 = 2$, $F_2 = 1$, and $F_1 = 1$, we get:

$$\begin{aligned} 3 &= 1 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 + 0. \end{aligned}$$

Hence, $\gcd(F_n, F_{n+1}) = 1$. □

(ii) Using 1(a)(i), prove that for $n \geq 1$, F_n and F_{n+2} are relatively prime.

Proof. Consider two Fibonacci numbers F_n and F_{n+2}. By the definition of the Fibonacci sequence, we have that,

$$F_{n+2} = F_n \cdot F_1 + F_2 \cdot F_{n-1}.$$

From this, we can see that,

$$\begin{aligned}\gcd(F_n, F_{n+2}) &= \gcd(F_n, F_n \cdot F_1 + F_2 \cdot F_{n-1}) \\ &= \gcd(F_n, F_n \cdot 1 + 1 \cdot F_{n-1}) \\ &= \gcd(F_n, F_{n-1})\end{aligned}$$

Since by 1(a)(i), F_n and F_{n-1} are relatively prime.
Hence, by 1(a)(i), $\gcd(F_n, F_{n-1}) = \gcd(F_n, F_{n+2}) = 1$. $\square$

(b) In class we observed the following about 4 consecutive Fibonacci numbers:
- Let x be the product of the first and fourth numbers.
- Let y be *twice* the product of the second and third numbers.
- Let z be the *sum* of the square of the second number with the square of the third number.

Then $x^2 + y^2 = z^2$, that is, (x, y, z) is a Pythagorean triple.
For example, for F_1, F_2, F_3, and F_4, we have:
- $x = F_1 \cdot F_4 = 1 \cdot 3 = 3$.
- $y = 2 \cdot F_2 \cdot F_3 = 2 \cdot 1 \cdot 2 = 4$.
- $z = F_2^2 \cdot F_3^2 = 1^2 \cdot 2^2 = 5$.

Please complete the following:

(i) Express the procedure described above in the form of a claim that can be proven via *mathematical induction* and then prove the claim by induction.

Claim. If F_n is a Fibonacci number, then,

$$(F_n \cdot F_{n+3}, 2F_{n+1} \cdot F_{n+2}, F_{n+1}^2 + F_{n+2}^2)$$

is a Pythagorean triple.

Proof. We will proceed by induction on n.
Base case: When $n = 1$, we know that $F_1 = F_2 = 1$, $F_3 = 2$, and $F_4 = 3$. So we have:

$$\begin{aligned}(F_1 \cdot F_4, 2F_2 \cdot F_3, F_2^2 + F_3^2) &= (1 \cdot 3, 2 \cdot 1 \cdot 2, 1^2 + 2^2) \\ &= (3, 4, 5)\end{aligned}$$

Which is clearly a Pythagorean triple, since $3^2 + 4^2 = 5^2$.

Inductive case: Assume the claim holds for F_k. We want to show it also holds for F_{k+1}. In other words, assuming that,

$$(F_k \cdot F_{k+3}, 2F_{k+1} \cdot F_{k+2}, F_{k+1}^2 + F_{k+2}^2)$$

is a Pythagorean triple, we want to show that,

$$(F_{k+1} \cdot F_{k+4}, 2F_{k+2} \cdot F_{k+3}, F_{k+2}^2 + F_{k+3}^2)$$

is also a Pythagorean triple.
This means that we need to show:

$$(F_{k+1} \cdot F_{k+4})^2 + (2F_{k+2} \cdot F_{k+3})^2 = (F_{k+2}^2 + F_{k+3}^2)^2.$$

Observe that:

$$(F_{k+1} \cdot F_{k+4})^2 + (2F_{k+2} \cdot F_{k+3})^2 = \dots$$

$$= F_{k+2}^4 + 2 \cdot F_{k+2}^2 \cdot F_{k+3}^2 + F_{k+3}^4$$
$$= (F_{k+2}^2 + F_{k+3}^2)^2$$

□

(ii) Under what conditions will (x, y, z) form a *primitive* Pythagorean triple? Your answer should be as specific as possible and should be connected to your claim in 1(b)(i).

Solution. We know that Pythagorean triples are generated by $(t^2 - s^2, 2st, t^2 + s^2)$, for all $s < t$. Similarly, we proved that a Pythagorean triple if one of s, t is even and the other is odd.
Since in the definition of Fibonacci Pythagorean triples the second term is $2 \cdot F_{n+1} \cdot F_{n+2}$, we can say that $s = F_{n+1}$ and $t = F_{n+2}$. Therefore, a Pythagorean triple generated this way is primitive if F_{n+1} and F_{n+2} are not both odd.
In other words, a Pythagorean triple generated by F_n is primitive if:

$$n \mod 3 \neq 0.$$

(2) *Defn.* Let (a, b, c) be a Pythagorean triple. We say that triple (a, b, c) is a FP triple if and only if (a, b, c) is produced by the procedure described 1(b)(i). Moreover for $n \geq 1$, let $FP(n)$, denote the FP-triple created by F_n, F_{n+1}, F_{n+2}, and F_{n+3}.

Thus, $FP(1) = (3, 4, 5)$ and $FP(2) = (5, 12, 13)$.

Defn. The FP triple (a, b, c) is PFP if and only if (a, b, c) is a *primitive* FP triple.

Defn. For $n \geq 1$, let,

$$C_n = \{FP(i) : 1 \leq i \leq n\}$$

and,

$$D_n = \{FP(i) : 1 \leq i \leq n \text{ and } FP(i) \text{ is } PFP\}$$

Answer the following:

(a) What is $|C_n|$, the cardinality of C_n?

Solution. By its definition, $|C_n| = n$.

(b) Give a formula for $|D_n|$.

Solution.

$$|D_n| = \left\lfloor \frac{2(n+1)}{3} \right\rfloor$$

(c) Determine:

$$\lim_{n\to\infty} \frac{|D_n|}{|C_n|}$$

Solution.

$$\lim_{n\to\infty} \frac{|D_n|}{|C_n|} = \lim_{n\to\infty} \frac{\left\lfloor \frac{2(n+1)}{3} \right\rfloor}{n} = \frac{2}{3}$$

(3) In class we considered the sequence of Fibonacci numbers *modulo* 10 and saw that this sequence repeated a pattern after 60 terms.

(a) If we consider the sequence of Fibonacci numbers *modulo* 8, what is the length of its repeated pattern?

Solution. The pattern ($\{1, 1, 2, 3, 5, 0, 5, 5, 2, 7, 1, 0\}$) has length 12.

(b) (i) What is the smallest n such that 30 divides F_n?

Solution. 1548008755920, the 60th Fibonacci number, is the smallest such that 30 divides it.

(ii) If we consider the sequence of Fibonacci numbers *modulo* 30, what is the length of its repeated pattern?

Solution. The length of the repeated pattern is 60.

(c) We know that $F_{15} = 610$. If we consider the sequence of Fibonacci numbers *modulo* 610, what is the length of its repeated pattern?

Solution. The pattern also has length 60.

(4) (a) A shopper spends a total of \$5.49 for oranges, which cost \$0.18 a piece, and grapefruits, which cost \$0.33 each. What is the *minimum* number of pieces of fruit that the shopper could have bought?

Solution. Consider the non-negative integer solutions to the following equation:

$$5.49 = 0.18O + 0.33G$$

The solutions are as follows:

- 3 oranges, 15 grapefruit.
- 14 oranges, 9 grapefruit.
- 25 oranges, 3 grapefruit.

The first solution has 18 total fruit, which is the minimum number of pieces that the shopper could have bought.

(b) An ancient chinese puzzle found in the 6th century work of the mathematician Chang Ch'iu-chien, called the "Hundred Foods" Problem asks:
If a cock is worth 5 coins, a hen 3 coins, and 3 chickens together are worth 1 coin, how many cocks, hens, and chickens totaling 100 can be bought for 100 coins?

Solution. Consider the non-negative integer solutions to the following equation:

$$100 = 5k + 3h + c = k + h + 3c$$

The solutions are as follows:

- 0 cocks, 25 hens, 75 chickens.
- 4 cocks, 18 hens, 78 chickens.
- 8 cocks, 11 hens, 81 chickens.
- 12 cocks, 4 hens, 84 chickens.

(5) Let $(R, +, \cdot)$ be a commutative ring.

(a) Prove that if I_1 and I_2 are *ideals* of R, then $I_1 \cap I_2$ is an ideal of R.

Proof. First we must show that $I_1 \cap I_2$ is an ideal of R. We know from a previous theorem that the intersection of two subgroups is a subgroup, so the intersection of I_1 and I_2 forms a subgroup.
Let $x \in I_1 \cap I_2$. If $y \in R$, then $x + y$ and $y + x$ are in both I_1 and I_2 and thus in $I_1 \cap I_2$. So $I_1 \cap I_2$ is an ideal of R. $\square$

(b) Let $A \subseteq R$.

Defn. The Annihilator of A, defined by,

$$Ann(A) = \{x \in R : a \cdot x = 0_R \ \forall a \in A\}$$

is a subset of R.

(i) Prove that $Ann(A)$ is an *ideal* of R.

Proof. If m, $n \in Ann(A)$, then so are $m - n$ and rm for all $r \in R$. Therefore $Ann(A)$ is a subring of R. By the distributive law, $Ann(A)$ is closed under addition and right multiplication.
Fix $x \in Ann(A)$ and $r \in R$. Select any $a \in A$. Then $ar \in A$, but then $(ar)x = 0$ because $x \in Ann(A)$. Therefore, $a(rx) = 0$ and $rx \in Ann(A)$. Thus, $Ann(A)$ is an ideal of R. □

(ii) Suppose that,

$$R = \mathbb{Z}_4 \times \mathbb{Z}_{100},$$

and,

$$Y = \{(0, 52), (2, 40)\}.$$

Determine $Ann(Y)$.

Solution.

$$Ann(Y) = \{(0, 0), (0, 25), (0, 50), (0, 75), (2, 0), (2, 25), (2, 50), (2, 75)\}$$

(iii) Suppose that $R = \mathbb{C}$ (where $\mathbb{C}$ is the ring of complex numbers with the usual addition and multiplication), and let,

$$W = \{1 + i, \sqrt{2} - i\}$$

Determine $Ann(W)$.

Solution.

$$Ann(W) = \{0\}$$

(6) Let $(R, +, \cdot)$ be a ring.

(a) Define $P : R[x] \to R$ as follows:

$$P(a_0 + a_1x + a_2x^2 + \ldots + a_nx^n) = a_0$$

(i) Prove that P is a *ring homomorphism* from $R[x]$ *onto* R.

Proof. We must show that:

$$P(a+b) = P(a) + P(b)$$

and,

$$P(ab) = P(a)P(b)$$

For all a, $b \in R$.

Let

$$a_0 + a_1x + \ldots + a_nx^n \in R[x],$$

and,

$$b_0 + b_1x + \ldots + b_nx^n \in R[x].$$

Then we have:

$$P(a_0 + a_1x + \ldots + a_nx^n + b_0 + b_1x + \ldots + b_nx^n)$$
$$= P[(a_0+b_0) + (a_1+b_1)x + \ldots + (a_n+b_n)x^n] = a_0 + b_0$$
$$= P(a_0 + a_1x + \ldots + a_nx^n) + P(b_0 + b_1x + \ldots + b_nx^n).$$

Also, we have:

$$P[(a_0 + a_1x + \ldots + a_nx^n) \cdot (b_0 + b_1x + \ldots + b_nx^n)]$$
$$= P[(a_0 \cdot b_0) + (a_1 \cdot b_0 + a_0 \cdot b_1)x + \ldots + (a_n \cdot b_0 + a_{n-1} \cdot b_1 + \ldots + (a_0 \cdot b_n)x^n]$$
$$= a_0 \cdot b_0 = P(a_0 + a_1x + \ldots + a_nx^n) \cdot P(b_0 + b_1x + \ldots + b_nx^n).$$

Finally, it is clear that the multiplicative identity in $R[x]$ maps to the multiplicative identity in R, since $P(1 + x + x^2 + \ldots + x^n) = 1$. □

(ii) What is $Ker(P)$?

Solution. $Ker(P) = \{a_0 + a_1x + \ldots + a_nx^n \in R[x] : a_0 = 0\}$

(iii) To what ring is $R[x]/Ker(P)$ isomorphic?

Solution. By the first isomorphism theorem, the image of $R[x]$ under P is isomorphic to $R[x]/Ker(P)$.

(b) Consider the derivative mapping:

$$D : R[a] \to R[a]$$

given by,

$$D(a_0 + a_1x + \ldots + a_nx^n) = a_1 + 2a_2x + \ldots + na_nx^{n-1}$$

(i) Prove D is a *group* homomorphism.

Proof. We must show that:

$$D(a+b) = D(a) + D(b)$$

and,

$$D(ab) = D(a)D(b)$$

For all a, $b \in R[a]$.

Let

$$a_0 + a_1x + \ldots + a_nx^n \in R[a],$$

and,

$$b_0 + b_1x + \ldots + b_nx^n \in R[a].$$

Then we have:

$$D(a_0 + a_1x + \ldots + a_nx^n + b_0 + b_1x + \ldots + b_nx^n)$$

$$= D[(a_0 + b_0) + (a_1 + b_1)x + \ldots + (a_n + b_n)x^n]$$

$$= (a_1 + b_1) + 2(a_2 + b_2)x + \ldots + n(a_n + b_n)x^n$$

$$= (a_1 + 2a_2x + \ldots + na_nx^n) + (b_1 + 2b_2x + \ldots + nb_nx^n)$$

$$= D(a_0 + a_1x + \ldots + a_nx^n) + D(b_0 + b_1x + \ldots + b_nx^n).$$

Also, we have:

$$D[(a_0 + a_1x + \ldots + a_nx^n) \cdot (b_0 + b_1x + \ldots + b_nx^n)]$$

$$= D[(a_0 \cdot b_0) + (a_1 \cdot b_0 + a_0 \cdot b_1)x + \ldots + (a_n \cdot b_0 + a_{n-1} \cdot b_1 + \ldots + (a_0 \cdot b_n)x^n]$$

$$= (a_1 \cdot b_0 + a_0 \cdot b_1) + 2(a_2 \cdot b_0 + a_1 \cdot b_1 + a_0 \cdot b_2)x + \ldots + n(a_n \cdot b_0 + a_{n-1} \cdot b_1 + \ldots + a_0 \cdot b_n)x^n$$

$$= (a_1 + 2a_2x + \ldots + na_nx^{n-1}) \cdot (b_1 + 2b_2x + \ldots + nb_nx^{n-1})$$

$$= D(a_0 + a_1x + \ldots + a_nx^n) \cdot D(b_0 + b_1x + \ldots + b_nx^n).$$

□

(ii) What is $Ker(D)$?

Solution. $Ker(D) = \{a_0 + a_1x + \ldots + a_nx^n \in R[a] : a_i = 0\, \forall i \geq 1\}$

(iii) Explain why D is *not* a *ring* homomorphism.

Solution. D is not a ring homomorphism because there is no mapping from the multiplicative identity in $R[a]$ to itself.

(iv) Is $D : \mathbb{Z}[a] \to \mathbb{Z}[a]$ *onto*? Justify your answer.

Solution. No. Recall that for D to be onto it must be true that for all $b \in R[a]$ there is an $a \in R[a]$ such that $D(a) = b$. Consider $b \in R[a]$ such that the x^1 term is odd. This element can never be mapped to by D, since by the definition of D the x^1 term must be even (since it is multiplied by 2).

(7) Refer to Section 3.8 on page 149 of your handout.
Find the greatest common divisor in $\mathbb{Z}[i]$ of $11 + 7i$ and $18 - i$. *Show work!*
Hint: Read carefully the proof of Theorem 3.8.1.

Solution. Recall the d function for the Gaussian integers is defined by:

$$d(a + bi) = a^2 + b^2 = (a + bi)(a - bi)$$

For $11 + 7i$ we have:

$$d(11 + 7i) = 11^2 + 7^2 = 170 = 2 \cdot 5 \cdot 17$$
$$11 + 7i = -i \cdot (1 + i) \cdot (1 + 2i) \cdot (4 + i)$$

For $18 - i$ we have:

$$d(18 - i) = 10^2 + 1^2 = 325 = 5^2 \cdot 13$$
$$18 - i = -i \cdot (2 + i)^2 \cdot (3 + 2i)$$

So the greatest common divisor in $\mathbb{Z}[i]$ is $-i$. But recall that the units of $\mathbb{Z}[i]$ are $\{1, -1, i, -i\}$. Therefore, $11 + 7i$ and $18 - i$ are relatively prime.