HOMEWORK 2
CHRIS POWELL
STARDATE 2019.37

1. A circular dial has the numbers 0 through 56 inscribed at equal intervals along the rim.

   (a) A grasshopper sits at the 0. It can jump 5 units in either direction (clockwise or counterclockwise) any number of times. What is the set of numbers that the grasshopper can reach with a sequence of jumps?

   The set of numbers the grasshopper can reach is $\{0, 1, \ldots, 56\}$.

   Claim. For each $n \in \mathbb{Z}$, there is some $k \in \mathbb{Z}$ for which $5k \equiv n \mod 57$.

   Proof. Since $\gcd(5, 57) = 1$, we know $\overline{5}$ is a unit in $\mathbb{Z}_{57}$. So there must be some $m \in \mathbb{Z}$ for which $5m \equiv 1 \mod 57$. Thus for any $n \in \mathbb{Z}$, we have $5m \cdot n \equiv 1 \cdot n$. But since $\mathbb{Z}$ is a ring, $mn = k$ for some $k \in \mathbb{Z}$ and $1 \cdot n = n$, so $5k \equiv n \mod 57$, as claimed. □

   The positions on the dial combined with the grasshopper's ability to jump is isomorphic to $\mathbb{Z}_{57}$. Consequently, the above result implies that the grasshopper can get to any position on the dial.

   (b) Same question, but instead the grasshopper can only jump 3 units at a time.

   Let $S = \{0, 1, \ldots, 56\}$. The set of numbers the grasshopper can reach is given by $\{x \in S \mid x \equiv 0 \mod 3\}$

   Claim. For each $m \in \mathbb{Z}$, there is some $n \in \mathbb{Z}$ for which $3m \equiv 3n \mod 57$.

   Proof. Let $m \in \mathbb{Z}$. Suppose otherwise that there is no $n \in \mathbb{Z}$ such that $3m \equiv 3n \mod 57$. Then either $3m \equiv 3n + 1 \mod 57$ or $3m \equiv 3n + 2 \mod 57$. If $3m \equiv 3n + 1 \mod 57$ for some $n \in \mathbb{Z}$, then $3(m - n) \equiv 1 \mod 7$, which implies 3 is a unit. But this is impossible since $\gcd(3, 57) = 3 \neq 1$. Now assume $3m \equiv 3n + 2 \mod 57$. Then $3(m - n) \equiv 2 \mod 57$. Since $\gcd(2, 57) = 1$, we know there must be some integer k satisfying $2k \equiv 1 \mod 57$. But then by transivitiy of the congruence relation, $3(m - n)k \equiv 1$, another contradiction. □

2. Silverman 2.1

   (a) We showed that in any primitive Pythagorean triple (a, b, c), either a or b is even. Use the same sort of argument to show that either a or b must be a multiple of 3.

Lemma. There exists no integer whose square is congruent to $2 \mod 3$.

Proof. Let $n \in \mathbb{Z}$. Then $n \equiv x \mod 3$ for exactly one $x \in \{0, 1, 2\}$. Suppose $n \equiv 0 \mod 3$. Then $n = 3k$ for some $k \in \mathbb{Z}$. So $n^2 = 9k^2 = 3(3k^2)$. Thus $n^2 \equiv 0 \mod 3$. Suppose $n \equiv 1 \mod 3$. Then $n = 3k + 1$ for some $k \in \mathbb{Z}$. So $n^2 = (3k + 1)^2 = 9k^2 + 6k + 1 = 3(3k^2 + 2k) + 1$. Hence, $n^2 \equiv 1 \mod 3$. Suppose $n \equiv 2 \mod 3$. Then $n = 3k + 2$ for some $k \in \mathbb{Z}$. So $n^2 = (3k + 2)^2 = 9k^2 + 6k + 4 = 3(3k^2 + 2k + 1) + 1$. Hence, $n^2 \equiv 1 \mod 2$. □

Claim. Let (a, b, c) be a primitive Pythatgorean triple. Then either a or b is a multiple of 3.

Proof. Suppose otherwise that 3 divides neither a nor b. Then $a^2 \equiv b^2 \equiv 1 \mod 3$ since $x^2 \not\equiv 2 \mod 3$ for any $x \in \mathbb{Z}$ by the above lemma. So $a^2 = 3m+1$ and $b^2 = 3n + 1$ for some $m, n \in \mathbb{Z}$. Since $\mathbb{Z}$ is a commutative ring, we have

$$c^2 = 3m + 1 + 3n + 1 = 3m + 3n + 2 = 3(m + n) + 2.$$

But this implies $c^2 \equiv 2 \mod 3$, a contradiction. □

(b) By examining the above list of primitive Pythagorean triples, make a guess about when a, b, or c is a multiple of 5. Try to show that your guess is correct.

Lemma. The square of any integer is congruent to 0, 1, or 4 mod 5.

Proof. Let $n \in \mathbb{Z}$. Then $n \equiv x \mod 5$ for exactly one $x \in \{0, \ldots, 4\}$. If $n \equiv 0 \mod 5$, then $n^2 = 0 \mod 5$. If $n \equiv 0 \mod 5$, then $n = 5m$ for some $m \in Z$. So $n^2 = 5k$ with $k = 5m^2$. If $n \equiv 1 \mod 5$, then $n = 5m + 1$ for some $m \in Z$. So $n^2 = 5k + 1$ with $k = 5m^2 + 2m$. If $n \equiv 2 \mod 5$, then $n = 5m + 2$ for some $m \in \mathbb{Z}$. So $n^2 = 5k + 4$ with $k = 5m^2 + 4m$. If $n \equiv 3 \mod 5$, then $n = 5m + 3$ for some $m \in \mathbb{Z}$. So $n^2 = 5k + 4$ with $k = 5m^2 + 6m + 1$. If $n \equiv 4 \mod 5$, then $n = 5m + 4$ for some $m \in \mathbb{Z}$. So $n^2 = 5k + 1$ with $k = 5m^2 + 8m + 3$. □

Claim. Let (a, b, c) be a Primitive Pythagorean Triple. Then exactly one of a, b or c is congruent to $0 \mod 5$.

Proof. Let (a, b, c) be a primitive Pythagorean triple. Then a and b can not both be congruent to $0 \mod 5$, as then $c \equiv 0 \mod 5$ which contradicts primivity of (a, b, c). Suppose neither a nor b is congruent $0 \mod 5$. If both a^2 and b^2 are congruent to $1 \mod 5$, then c^2, and thus c, is congruent to $0 \mod 5$, which contradicts the above lemma. Similarly, it cannot be that both a^2 and b^2 are congruent to $4 \mod 5$, otherwise $c^2 = 3 \mod 5$, another contradiction. So if neither a nor b is congruent to $0 \mod 5$, then one of a^2 and b^2 must be congruent to $1 \mod 5$, and the other congruent to $4 \mod 5$. Thus $c^2 \equiv 0 \mod 5$ which implies $c \equiv 0 \mod 5$. Now suppose neither b nor c is congruent to $0 \mod 5$. We show $a \equiv 0 \mod 5$. Note that $a^2 = c^2 - b^2$. If $c^2 = 1 \mod 5$ and $b^2 \equiv 1 \mod 5$, then $a^2 = 0 \mod 5$, and thus $a \equiv 0 \mod 5$. If both c^2 and b^2 are congruent to $4 \mod 5$, then $a^2 \equiv 0 \mod 5$. If $c^4 \equiv 4 \mod 5$ and $b^2 \equiv 1 \mod 5$, then $a^2 = 3 \mod 5$, a contradiction. If $c^2 = 1 \mod 5$ and $b^2 \equiv 4 \mod 5$, then $a^2 = 2 \mod 5$ and thus $a \equiv 2 \mod 5$, which is impossible. Therefore if neither b nor c is congruent to 0 mod 5, then a must be. The result follows. □

3. Silverman 2.5

In Chapter 1 we saw that the n^{th} triangular T_n is given by the formula

$$T_n = 1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}.$$

The first few triangular numbers are 1, 3, 6, and 10. In the list of the first few Pythagorean triples (a, b, c), we find $(3, 4, 5)$, $(5, 12, 13)$, $(7, 24, 25)$, and $(9, 40, 41)$. Notice that in each case, the value of b is four times a triangular number.

(a) Find a primitive Pythagorean triple (a, b, c) with $b = 4T_5$. Do the same for $b = 4T_6$ and for $b = 4T_7$.

By applying the result from part (b) of this exercise, we get the following as the required Primitive Pythagorean Triples:
$(a, 4T_5, c) = (11, 60, 61)$
$(a, 4T_6, c) = (13, 84, 85)$
$(a, 4T_7, c) = (15, 112, 113)$

(b) Do you think that for every triangular number T_n, there is a primitive Pythagorean triple (a, b, c) with $b = 4T_n$? If you believe that this is true then prove it. Otherwise, find some triangular number for which it is not true.

Yes.

Claim. The triple $(a, b, c) = \big(2n+1, 4T_n, 2n^2+2n+1\big)$ yields a Primitive Pythagorean Triple for all $n \in \mathbb{N}_{>0}$.

Proof. Let T_n be the nth triangular number, where $n \in \mathbb{N}_{>0}$. Then $4T_n = 2n(n+1)$ since $T_n = \frac{n(n+1)}{2}$. Set $s = 2n+1$ and $t = 1$. Then s and t are odd integers satisfying $s > t \geq 1$. Also, s and t must be relatively prime; otherwise, their common factor would divide both $n+1 = \frac{s+t}{2}$ and $n = \frac{s-t}{2}$, contradicting the fact that $\gcd(n, n+1) = 1$. Now observe that $st = (2n+1)\cdot 1 = 2n+1$, $4T_n = 2n(n+1) = \frac{s^2-t^2}{2}$, and $(n+1)^2 + 1^2 = \frac{s^2+t^2}{2}$. Therefore, by Theorem 1, $\big(2n+1, 4T_n, 2n^2+2n+1\big)$ is a Primitive Pythagorean Triple. □

4. Silverman 3.2

(a) Use the lines through the point $(1, 1)$ to describe all the points on the circle $x^2 + y^2 = 2$ whose coordinates are rational numbers.

Let ℓ be the line passing through point $(1, 1)$. Then the equation for ℓ is given by $y - 1 = m(x-1)$ which implies $y = mx - m + 1$. Now observe that

$$\begin{aligned} x^2 + y^2 &= 2 \\ x^2 + (mx - m + 1)^2 &= 2 \\ x^2 + m^2x^2 + m^2 + 1 - 2m^2x - 2m + 2mx &= 2 \\ (m^2+1)x^2 - 2(m^2-m)x + (m^2 - 2m - 1) &= 0 \end{aligned}$$

Then dividing $(m^2+1)x^2 - 2(m^2-m)x + (m^2-2m-1)$ by $x - 1$, we obtain

$$(m^2+1)x - (m^2 - 2m - 1)$$

So

$$x = \frac{m^2 - 2m - 1}{m^2 + 1}$$

Thus

$$y = m\left(\tfrac{m^2-2m-1}{m^2+1}\right) - m + 1 = \tfrac{-m^2-2m+1}{m^2+1}$$

Hence $(x, y) = \left((m^2+1)x - (m^2-2m-1), \frac{-m^2-2m+1}{m^2+1}\right)$.

5. Silverman 5.1

Use the Euclidean algorithm to compute each of the following gcd's.

(a) $\gcd(12345, 67890)$

$$\begin{aligned}
\gcd(12345, 67890) &= \gcd(12345, 67890 - 5(12345)) \\
&= \gcd(12345, 6165) \\
&= \gcd(12345 - 2(6165), 6165) \\
&= \gcd(15, 6165) \\
&= \gcd(15, 6165 - 411(15)) \\
&= \gcd(15, 0) \\
&= 15
\end{aligned}$$

(b) $\gcd(54321, 9876)$

$$\begin{aligned}
\gcd(54321, 9876) &= \gcd(54321 - 5(9875), 9876) \\
&= \gcd(4941, 9876) \\
&= \gcd(4941, 9875 - 1(4941)) \\
&= \gcd(4941, 4935) \\
&= \gcd(4941 - 1(4935), 4935) \\
&= \gcd(6, 4935) \\
&= \gcd(6, 4935 - 822(6)) \\
&= \gcd(6, 3) \\
&= \gcd(6 - 2(3), 3) \\
&= \gcd(0, 3) \\
&= 3
\end{aligned}$$

6. Silverman 5.6 The proof should be very short!

Write a program to implement the $3n + 1$ algorithm described in the previous exercise. The user will input n and your program should return the length $L(n)$ and the previous terminating value $T(n)$ of the $3n+1$ algorithm. Use your program to create a table giving the length and terminating value for all starting values $1 \leq n \leq 100$.

```
def g(n):
    """Compute Length of Termination and Terminating value"""
    A, i = [], 0
    while n not in A:
        A, i = A + [n], i + 1
        if n % 2 == 0:
            n = n // 2
        else:
            n = (3 * n) + 1
    return i, A[i-1]


def f(k):
    """Print table for Length of Termation and Terminating values"""
    for n in range(1, k+1):
        print(n, g(n))
```

APPENDIX

$3n + 1$ algorithm output

```
1 (3, 2)
2 (3, 4)
3 (8, 1)
4 (3, 1)
5 (6, 1)
6 (9, 1)
7 (17, 1)
8 (4, 1)
9 (20, 1)
10 (7, 1)
11 (15, 1)
12 (10, 1)
13 (10, 1)
14 (18, 1)
15 (18, 1)
16 (5, 1)
17 (13, 1)
18 (21, 1)
19 (21, 1)
20 (8, 1)
21 (8, 1)
22 (16, 1)
23 (16, 1)
24 (11, 1)
25 (24, 1)
26 (11, 1)
27 (112, 1)
28 (19, 1)
29 (19, 1)
30 (19, 1)
31 (107, 1)
32 (6, 1)
33 (27, 1)
34 (14, 1)
35 (14, 1)
36 (22, 1)
37 (22, 1)
38 (22, 1)
39 (35, 1)
40 (9, 1)
41 (110, 1)
42 (9, 1)
43 (30, 1)
44 (17, 1)
45 (17, 1)
46 (17, 1)
47 (105, 1)
48 (12, 1)
49 (25, 1)
50 (25, 1)
51 (25, 1)
52 (12, 1)
53 (12, 1)
```

```
54 (113, 1)
55 (113, 1)
56 (20, 1)
57 (33, 1)
58 (20, 1)
59 (33, 1)
60 (20, 1)
61 (20, 1)
62 (108, 1)
63 (108, 1)
64 (7, 1)
65 (28, 1)
66 (28, 1)
67 (28, 1)
68 (15, 1)
69 (15, 1)
70 (15, 1)
71 (103, 1)
72 (23, 1)
73 (116, 1)
74 (23, 1)
75 (15, 1)
76 (23, 1)
77 (23, 1)
78 (36, 1)
79 (36, 1)
80 (10, 1)
81 (23, 1)
82 (111, 1)
83 (111, 1)
84 (10, 1)
85 (10, 1)
86 (31, 1)
87 (31, 1)
88 (18, 1)
89 (31, 1)
90 (18, 1)
91 (93, 1)
92 (18, 1)
93 (18, 1)
94 (106, 1)
95 (106, 1)
96 (13, 1)
97 (119, 1)
98 (26, 1)
99 (26, 1)
100 (26, 1)
```

E-mail address: powel054@cougars.csusm.edu