Homework 2

(Fundamental Theorem of Arithmetic, distribution of primes, primality testing, modular arithmetic)

Due Wednesday, October 2 at 11:30am in class.

Note: Be sure to justify your answers. No credit will be given for answers without work/justification. In addition, all written homework assignments should be neat and well-organized; **this assignment has only one part and can be submitted as a single packet**.

(1) Consider the set of even integers $\mathbb{E}$. Let $a, b \in \mathbb{E}$. We say that a $\mathbb{E}$–divides b if there exists $c \in \mathbb{E}$ such that $ac = b$. An element p of $\mathbb{E}$ is called $\mathbb{E}$–prime if there is no element in $\mathbb{E}$ which $\mathbb{E}$–divides p. The following is a list of some $\mathbb{E}$–primes:

$$2, 6, 10, 14, 18, \ldots$$

(a) Describe all $\mathbb{E}$–primes.

An even integer p is $\mathbb{E}$–prime if and only if $2^1 \mid\mid p$.

(b) Suppose that $a, b \in \mathbb{E}$ and p is an $\mathbb{E}$–prime. Show, via a counterexample, that the following statement does *not* hold:

"If p $\mathbb{E}$–divides ab, then p $\mathbb{E}$–divides a or p $\mathbb{E}$–divides b."

For example, let $a = 10$, $b = 18$, and $p = 6$. Then 6 $\mathbb{E}$–divides 180, but 6 does not $\mathbb{E}$–divide 10 or 18.

(c) Prove that every positive element in $\mathbb{E}$ has a prime factorization.

Proof. Let n be a positive number in $\mathbb{E}$. We will use strong induction on n. First, note that $n = 2$ is its own prime factorization, so the base case holds. Now, suppose that all of the numbers $2, 4, 6, 8, \ldots, n$ have a prime factorization. If $n + 2$ is an $\mathbb{E}$–prime, we are done. If $n+2$ is not an $\mathbb{E}$–prime, then by definition, there is an element m in $\mathbb{E}$ which $\mathbb{E}$–divides $n + 2$. Since m $\mathbb{E}$–divides $n + 2$, it follows that $m < n + 2$ and $(n + 2)/m < n + 2$ and so by our induction hypothesis, both m and $(n + 2)/m$ have factorizations into $\mathbb{E}$–primes. Thus their product $n + 2 = m \cdot (n + 2)/m$ has a factorization into $\mathbb{E}$–primes. □

(d) Show, via a counterexample, that prime factorization in $\mathbb{E}$ is not unique.

For example, $36 = 2 \times 18 = 6 \times 6$.

(2) (a) For which primes p is p^2+2 also prime?
Only for $p=3$. If $p \neq 3$, then $p = 3q \pm 1$ for some integer q. Then we have

$$p^2+2 = (3q \pm 1)^2 + 2 = 9q^2 \pm 6q + 3 = 3(3q^2 \pm 2q + 1),$$

and p^2+2 is divisible by 3 (not prime).

(b) Show that if $p > 1$ and p divides $(p-1)!+1$, then p is prime.

Proof. Suppose that $p > 1$ and p divides $(p-1)!+1$. Rearranging, we have that

$$(p-1)! - pq = 1.$$

This implies that each of the equations

$$\begin{aligned} 2x + py &= 1 \\ 3x + py &= 1 \\ 4x + py &= 1 \\ &\vdots \\ (p-1)x + py &= 1 \end{aligned}$$

has a solution. (Specifically, $x = (p-1)!/2, (p-1)!/3, \ldots$ and $y = -q$.) Thus, p is coprime to $2, 3, 4, \ldots, p-1$ and so is prime. □

(c) Suppose that a positive integer n has k 0s at the end of its decimal expansion. (For example, if $n = 3100$, then $k = 2$.) What can you say about e, where $2^e \mid\mid n$?
$e \geq k$ since each 0 represents a factor of $10 = 2.5$ in n.

(3) (a) Without using a calculator, find:

(i) the least non-negative residue of $30 \times 27 \mod (13)$.
Since $30 \equiv 4$ and $27 \equiv 1 \bmod 13$, then $30 \times 27 \equiv 4 \times 1 \equiv 4 \bmod 13$.

(ii) the least absolute residue of $82 \times 63 \mod (55)$.
Since $82 \equiv 27$ and $63 \equiv 8$, we have that $82 \times 63 \equiv 27 \times 8 = (27 \times 2) \times 4 = 54 \times 4 \equiv -1 \times 4 = -4 \bmod 55$.

(iii) the remainder when 10^9 is divided by 7.
We have that

$$\begin{aligned} 10 &\equiv_7 3 \\ 10^2 &\equiv_7 3^2 \equiv_7 2 \\ 10^8 = (10^2)^4 &\equiv_7 2^4 = 16 \equiv_7 2 \\ 10^9 = 10^8 \cdot 10 &\equiv_7 2 \cdot 3 = 6. \end{aligned}$$

So the remainder is 6.

(iv) the final decimal digit of $2! + 4! + 6! + \cdots 12!$.
We need to find the remainder when divided by 10. First note that 12! and 10! have remainder 0 when divided by 10. Since 6! and 8! both have factors of 5 and 2, they also have remainder 0 when divided by 10. For the remaining terms:

$$2! = 2 \equiv_{10} 2$$
$$4! = 24 \equiv_{10} 4$$

So the last digit of $2! + 4! + 6! + \cdots 12!$ is $2 + 4 = 6$.

(b) Find and prove a divisibility rule for 7.
(Hint: Consider the powers of 10 modulo 7. Can you find a pattern?)

Theorem 1. To determine if a positive integer a is divisible by 7, mutliply each of its digits right to left by

$$1, 3, 2, 6, 4, 5, 1, 3, 2, 6, 4, 5, 1, \ldots$$

respectively and add. If the result is divisible by 7, then so is a.

Proof. First, note that

$$\begin{aligned}
10 &\equiv_7 3 \\
10^2 &\equiv_7 3^2 \equiv_7 2 \\
10^3 &= 10 \cdot 10^2 \equiv_7 3 \cdot 2 = 6 \\
10^4 &= (10^2)^2 \equiv_7 2^2 = 4 \\
10^5 &= 10^4 \cdot 10 \equiv_7 4 \cdot 3 = 12 \equiv_7 5 \\
10^6 &= (10^2)^3 \equiv_7 2^3 = 8 \equiv_7 1 \\
10^7 &= 10^6 \cdot 10 \equiv_7 1 \cdot 3 = 3
\end{aligned}$$

Then for each positive integer k, let $k = 6q + r$ with $0 \leq r < 6$ as in the division algorithm. Then we have that $10^k = 10^{6q+r} = (10^6)^q 10^r \equiv_7 1^q 10^r = 10^r$, where $r = 0, 1, 2, 3, 4, 5$.
Let a be a positive integer and write

$$a = a_0 + a_1 10 + a_2 10^2 + a_3 10^3 + a_4 10^4 + a_5 10^5 + a_6 10^6 + \cdots + a_k 10^k.$$

Then

$$a \equiv_7 a_0 + 3a_1 + 2a_2 + 6a_3 + 4a_4 + 5a_5 + a_6 + \cdots + ra_k,$$

where $k = 6q + r$ as in the division algorithm. □

Fun problem (will not be graded): The Fibonacci sequence is given by $F_n = F_{n-1} + F_{n-2}$ where $F_0 = F_1 = 1$. For example, the first several terms in the sequence are

$$1, 1, 2, 3, 5, 8, 13, \ldots.$$

Use strong induction to show that there is a closed formula for the nth Fibonacci number, namely

$$F_n = \frac{1}{\sqrt{5}} \left(\left(\frac{1+\sqrt{5}}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right).$$