Winter 2021 MTH 440/540 Homework 1
Wyatt Whiting

1. For each pair a and b, find $q, r \in \mathbb{Z}$ with $a = qb + r$ and $0 \le r < b$.

(a) $a = 64$ and $b = 11$
$64 = 11 \cdot 5 + 9 \implies q = 11, r = 9$

(b) $a = -50$ and $b = 7$
$-50 = 7 \cdot -8 + 6 \implies q = -8, r = 6$

(c) $a = 91$ and $b = 13$
$91 = 13 \cdot 7 + 0 \implies q = 7, r = 0$

(d) $a = 11$ and $b = 15$
$11 = 15 \cdot 0 + 11 \implies q = 0, r = 11$

2. Prove that $6 \mid n^3 - n$ for all integers n. [Hint: First check it for $0 \le n \le 5$. Then reduce to this case by dividing n by 6 with remainder.]

We begin by checking case $n = 1$. We then have $n^3 - n = 1^3 - 1 = 0$, and cleary $6|0$ because $0 = 6 \cdot 0 + 0$.
We now perform an inductive step. Assume $6|n^3 - n$ for some $n \in \mathbb{N}$. Now, we may rearrange the expression as such:

$$(n+1)^3 - (n+1) = n^3 + 3n^2 + 3n + 1 - n - 1 = (n^3 - n) + 3n(n+1)$$

We know the product $n(n+1)$ must be even since either n or $n+1$ must be even, so $2|n(n+1)$. Additionally, 3 clearly divides $3n(n+1)$ since $3n(n+1) = 3 \cdot (n(n+1))$. Therefore, since both 2 and 3 are factors of $3n(n+1)$, then $6|3n(n+1)$. We then have $6|n^3 - n$ by the induction hypothesis and $6|3n(n+1)$. Therefore, 6 must also divide the sum $(n^3 - n) + 3n(n+1) = (n+1)^3 - (n+1)$. We have therefore shown that $6|n^3 - n \implies 6|(n+1)^3 - (n+1)$. By the principle of induction, $6|n^3 - n$ for all $n \in \mathbb{N}$.
Now, let $a, b \in \mathbb{Z}$ be such that $a|b \implies b = ka$ for some $k \in \mathbb{Z}$. We can then also say that $a|-b$, as we can choose $m = -k$ so that $-b = ma = -ka$. We have already demonstrated that $6|n^3 - n$ for all positive integers n. $n^3 - n$ is an odd function, so if $n^3 - n = p$, then $(-n)^3 - (-n) = -p$. Therefore, if $6|n^3 - n \implies 6|p$, then it must also be the case that $6|-p \implies 6|(-n)^3 - (-n)$ for all $n \in \mathbb{N}$.
Now we just need to check the case for $n = 0$, which is trivially true, as $0^3 - 0 = 0 = 0 \cdot 6$, so $6|0$.
We have then shown that $6|n^3 - n$ and $6|(-n)^3 - (-n)$ for all $n \in \mathbb{N}$, which together constitute all non-zero integers. Together with the case of $n = 0$, we have proven that $6|n^3 - n$ for all integers. ☠

3. The first few primes of the form $6x+5$ (for $x \in \mathbb{Z}$) are $5, 11, 17, 23, 29, 41, 47, 53, 59, 71, \ldots$. In this problem you will show that there are infinitely many primes of the form $6x + 5$.

(a) Let p be a prime number which is not 2 or 3. Show that when p is divided by 6, the remainder is either 1 or 5.

Let p be an arbitrary prime greater than 3. If we divide p by 6 with remainder, we can express it in the form $p = 6 \cdot q + r$ for some $q \in \mathbb{Z}$ with $0 \le r < 6$. The remainder r cannot be 0, 2, or 4, since this would make $6 \cdot q + r$ an even number, which would contradict our assumption that p is prime. Likewise, the remainder cannot be 3, because $6 \cdot q + 3 = 3(2 \cdot q + 1)$ has 3 as a factor, which would contradict our assumption of p's primality. Since r cannot be 0, 2, 3, or 4, it must be the case that either $r = 1$ or $r = 5$.

(b) Show that the product of two numbers of the form $6x + 1$ is also of the form $6x + 1$.

Let $6x + 1$ and $6y + 1$ be such that $x, y \in \mathbb{Z}$. If we take the product of these two terms, we get

$$(6x + 1)(6y + 1) = 36xy + 6x + 6y + 1 = 6(6xy + x + y) + 1.$$

The integers are closed both under multiplication and addition, so the term $6xy + x + y$ must also be an integer. Therefore, the product of two numbers of the form $(6x + 1)$ where $x \in \mathbb{Z}$ must also be of the form $(6x + 1)$ for some $x \in \mathbb{Z}$.

(c) Show that if k is a positive integer, then $6k + 5$ has a prime factor p of the form $p = 6x + 5$.

We begin by noting $6k+5$ will always be odd, so 2 cannot be a factor. Additionally $6k + 5 = 3(2k + 1) + 2$, so 3 does not divide $6k + 5$ either and cannot be a factor. By the proof in section 3a, any prime factor must either be of the form $6x + 1$ or $6x + 5$. If $6k + 5$ has a prime factor of the form $6x + 5$, then we can take $x = k$ to form that factor. We now consider the case if $6k + 5$ has a prime factor of the form $6k + 1$ and not one in the from $6k + 5$. Since now $6k + 5$ must be composite, it must have at least two prime factors, both of which are in the form $6x + 1$. But from the proof in 3b, the product of these two factors would also be of the form $6x + 1$, which cannot be the case since we are only considered numbers of the form $6k + 5$. Therefore, it cannot have any prime factors of the forms $6x+1$, so $6k+5$ must have a prime factor of the form $6x + 5$.

(d) Modify Euclid's proof to show[1] that there are infinitely many primes of the form $6x + 5$.

Suppose there are only finitely many primes of the form $6x + 5$, enumerated in the set $\{p_1, p_2, \cdots, p_n\}$. Consider the value $q = 6p_1p_2 \cdots p_3 - 1 = 6(p_1p_2 \cdots p_n - 1) + 5$. By construction, no p_i divides q. By section 3a, any prime divisors of q must have the form $6x + 1$ or $6x + 5$. By section 3c, q must have at least one factor of the form $6x + 5$. If this were not the case, all prime factors of q would be in the form $6x + 1$, and by section 3b q would also be of the from $6x + 1$. However, the result that q must have at least one prime factor in the form $6x + 5$ contradicts the construction of q, which guarantees no prime of the form $6x + 5$ may factor it. Therefore, our assumption of the finiteness of primes in the from $6k + 5$ must be incorrect, so we may conclude there are infinitely many primes of the form $6x + 5$. ☠

4. In class we proved this theorem:

Theorem: Let a and b be integers (not both zero). Then $\gcd(a, b) = 1$ if and only if $ax + by = 1$ for some integers x and y.

[1] It is also true that there are infinitely many primes of the form $6x + 1$, but this is harder to show.

Using this theorem, prove the following statements. (Do not use the Fundamental Theorem of Arithmetic.) Here a, b, c are nonzero integers.

(a) Show that if $\gcd(a, b) = 1$ and $a \mid c$ and $b \mid c$, then $ab \mid c$.

We know there exist some x, y such that $ax + by = 1 \implies cax + cby = c$. Since $a|c \implies c = na$ and $b|c \implies c = mb$ for some m and n, we can then say that $mbax + naby = c \implies ab(mx + ny) = c \implies ab|c$ because $(mx + ny) \in \mathbb{Z}$ is an integer.

(b) Show that if $\gcd(a, b) = 1$ and $a \mid bc$, then $a \mid c$.

We know there exist some x, y such that $ax + by = 1 \implies cax + cby = c$. We also have $a|bc \implies bc = na$ for some n. Thus, $cax + nay = c \implies a(cx + ny) = c$, and because $(cx + ny)$ is an integer it must be the case that $a|c$.

(c) Show that if p is a prime number and $p \mid ab$, then either $p \mid a$ or $p \mid b$.

Since p is prime, we have $\gcd(p, a) = 1 \implies px+ay = 1$ and $\gcd(p, b) = ps+bt = 1$ for some integers x, y, s, t. We also have $p|ab \implies p = n \cdot ab$ for some integer n. We can multiply both sides of $px + ay = 1$ by b to obtain $bpx + bay = b$. The first term on the left is divisible by p, and by assumption $ab = ba$ is divisible by p, so the sum $bpx + bay = b$ is divisible by p, and therefore $p|b$.

We may do the same starting with the other equation: $ps+bt = 1 \implies psa+abt = a$, and we know $p|psa$ and $p|abt$ by the same reasoning above, so it must be the case that $p|(psa + abt) \implies p|a$.

We then conclude that either $p|a$ or $p|b$.

(d) Show that $\gcd(6x + 5, 5x + 4) = 1$ for all $x \in \mathbb{Z}$.

To demonstrate this, I will carry out Euclid's algorithm. Let $x \in \mathbb{Z}$ be arbitrary.

$6x + 5 = 1 \cdot (5x + 4) + (x + 1)$

$5x + 4 = 4 \cdot (x + 1) + x$

$x + 1 = 1 \cdot (x) + 1$

$x = x \cdot (1) + 0$

In the step before obtaining a remainder 0, we have remainder 1, which is then the greatest common divisor. We can then see that $\gcd(6x + 5, 5x + 4) = 1 \ \forall x \in \mathbb{Z}$.

5. For each pair a and b, use Euclid's algorithm to find $d = \gcd(a, b)$ and find $x, y \in \mathbb{Z}$ such that $ax + by = d$.

(a) $a = -23$ and $b = 16$ $-23 = -2 \cdot 16 + 9$

$16 = 1 \cdot 9 + 7$

$9 = 1 \cdot 7 + 2$

$7 = 3 \cdot 2 + 1$

$2 = 2 \cdot 1 + 0$

So $\gcd(-23, 16) = 1$. If we take $x = 9, y = 13$, we see that $-23 \cdot 9 + 16 \cdot 13 = 1$.

(b) $a = 111$ and $b = 442$

$442 = 3 \cdot 111 + 109$

$111 = 1 \cdot 109 + 2$

$109 = 54 \cdot 2 + 1$

$2 = 2 \cdot 1 + 0$

So $\gcd(111, 442) = 1$. If we take $x = 223, y = -56$, we see that $111 \cdot 223 + (-56) \cdot 442 = 1$.

6. Use Sage's `is_prime()` command to find the answers to the following questions. You may wish to use (suitably modified) versions of the programs on Homework 0 (the Sage warm-up).

(i) How many three-digit primes are there?

```
n = 0
for i in range(100, 1000):
    if is_prime(i):
        n = n + 1
print(n)

>143
```

There are 143 3-digit primes

(ii) List the three smallest ten-digit primes.

```
n = 0
p = 1000000001 # start with first ten-digit odd number
while n < 3:
    if is_prime(p):
        print(p)
        n = n + 1
    p = p + 2 # only check odd numbers since no evens will be prime

> 1000000007
> 1000000009
> 1000000021
```

The three numbers above are the three smallest 10-digit primes

(iii) Some primes[2] have the form $n^2 + 1$, such as $1^2 + 1 = 2$, $2^2 + 1 = 5$, and $4^2 + 1 = 17$. List all four-digit primes of the form $n^2 + 1$. How many are there?

```
for n in range(32, 99): # n^2 + 1 guaranteed to be 4-digit
    if is_prime(n*n + 1):
        print(n*n + 1)

> 1297
> 1601
> 2917
> 3137
> 4357
> 5477
```

[2]Nobody knows whether there are infinitely many primes of the form $n^2 + 1$.

```
> 7057
> 8101
> 8837
```

There are 9 4-digit primes of the form $n^2 + 1$.