Math 580 Homework.

1. Divisibility.

Definition 1. Let a, b be integers with $a \neq 0$. Then b ***divides*** b iff there is an integer k such that $b = ka$. In the case we write $a \mid b$. In this case we also say a is a ***factor*** of b, and that b is a ***multiple*** of a. □

Note that for any $a \neq 0$ we have $0 = 0 \cdot a$ and therefore 0 is a multiple of every nonzero integer. Likewise $a = 1 \cdot a$ and thus 1 is a factor of every nonzero integer.

We use the notation $a \nmid b$ if a does not divide b. Thus

$$2 \mid 18, \quad -4 \mid 24, \quad 19 \mid 133, \quad 5 \nmid 23, \quad 10 \nmid 4671, \quad 13 \nmid -50.$$

Example 2. If $a \mid b$ and $a \mid c$, then $a \mid (2b - 7c)$.

Proof: As $a \mid b$ there is an integer k such that $b = ka$. Likewise $a \mid c$ implies there is an integer ℓ such that $c = \ell a$. Then

$$2b - 7c = 2ka - 7\ell a = (2k - 7\ell)a = ka$$

where $k = (2k - 7\ell)$ is an integer. Thus $a \mid (2k - 7\ell)$. □

There was nothing special about 2 and -7:

Proposition 3. *Let $a \mid b$ and $a \mid c$. Then for any integers m and n we have $a \mid (mb + nc)$.*

Problem 1. Prove this. □

More generally

Proposition 4. *If $a \mid b_j$ for $j = 1, 2, \ldots, n$ and $m_1, m_2, \ldots, m_n$ are any integers then*

$$a \mid (m_1 b_1 + m_2 b_2 + \cdots m_n b_n).$$

Problem 2. Prove this. □

The next proposition is only of interest as a example of a proof involving divisibility.

Proposition 5. *If $a \mid b$, then $2a^2 \mid (4b^2 + 2b^3)$.*

Proof. As $a \mid b$ there is an integer k such that $b = ka$. Therefore

$$4b^2 + 2b^3 = 2(ak)^2 + 4(ak)^3 = 2a^2k^2 + 4a^3k^3 = 2a^2(k^2 + 2ak^3).$$

Therefore $4b^2 + 2b^3 = 2ak'$ where $k' = (k^2 + 2ak^3)$ is an integer. Whence $2a^2 \mid (4b^2 + 2b^3)$ □

As variants on this do the following.

Problem 3. Prove the following:
(a) If $a \mid b$, then $3a^3 \mid (9b^4 + 6ab^2)$.
(b) If $a \mid b$ and $a \mid c$, then $5a^2 \mid (15b^2 + 25c^2)$.

(c) If $a \mid x$ and $b \mid y$, then $3ab^2 \mid (-3aby + 9bx^4y)$. □

Here are some more basic properties if divisibility.

Proposition 6. *If $a \mid b$ and $b \mid c$, then $a \mid c$.*

Problem 4. Prove this. *Hint:* You should start by saying there are integers m and n such that $b = ma$ and $c = nb$. □

Proposition 7. *If $a \mid b$ then for any integer c we have $a \mid bc$.*

Problem 5. Prove this. □

Proposition 8. *If $a \mid x$ and $b \mid y$. Then $ab \mid xy$.*

Problem 6. Prove this. □

Proposition 9. *If $ab \mid ac$ and $a \neq 0$, then $b \mid c$.*

Problem 7. Prove this. □

Here is a less obvious divisibility result.

Proposition 10. *For any integer n we have*

$$2 \mid n(n-1).$$

Proof. First assume that $n \geq 2$ and let $q = \binom{n}{2}$. As the binomial coefficients are integers we have that

$$q = \binom{n}{2} = \frac{n(n-1)}{2}$$

is an integer. It follows that

$$n(n-1) = 2q$$

and so $n(n-1)$ has a factor of 2 when $n \geq 0$.

If $n \leq -1$, then then $-n \geq 1$ and so $-n + 1 \geq 2$. So if $m = -n + 1$ then, by what we have just done, $m(m+1)$ has a factor of 2. But

$$m(m-1) = (-n+1)(-n+1-1) = n(n-1).$$

So $n(n-1)$ has a factor of 2 when $n \leq -1$.

This covers all cases except $0 \leq n \leq 1$. So only $n = 0$ and $n = 1$ are left. But

$$0(0-1) = 0, \qquad 1(1-1) = 0$$

and 0 is divisible by 2. So $2 \mid n(n-1)$ for all $n \in \mathbb{Z}$. □

Problem 8. Show that $n(n-1)(n-2)$ is divisible by 6. *Hint:* Start with the case $n \geq 3$ and use that the binomial coefficient $\binom{n}{3}$ is an integer, which shows $6 \mid n(n-1)(n-2)$ for $n \geq 3$. If $n \leq -1$, then we can write

$$\begin{aligned} n(n-1)(n-2) &= (-1)^3(-n)(-n+2)(-n+3) \\ &= -(-n+3)(-n+2)(-n+1) \\ &= -m(m-1)(m-2) \end{aligned}$$

where $m = -n + 2$. Because $n \leq -1$ we have $m \geq 3$ and therefore $6 \mid m(m-1)(m-2)$ by what we have just done. Thus $n(n-1)(n-2) = -m(m-1)(m-2)$ id divisible by 6 where $n \leq -1$. This leaves the cases $n = 0, 1, 2$ which can be done by direct calculation. □

As all the binomial coefficients $\binom{n}{k}$ are integers it has probably occurred to you that something more general holds:

Proposition 11. *For any positive integer k and any integer n $k!$ divides the falling power $n^{\underline{k}} = n(n-1)(n-2)\cdots(n-k+1)$. That is*

$$k! \mid n(n-1)(n-2)\cdots(n-k+1)$$

Problem 9. Prove this. *Hint:* This is very like the last problem. When $n \geq k$ use that the binomial coefficient $\binom{n}{k}$ is an integer. Show for any n show that

$$\begin{aligned} n^{\underline{k}} &= n(n-1)(n-2)\cdots(n-k+2)(n-k+1) \\ &= (-1)^k(-n+k-1)(-n+k-2)\cdots(n-1)n \\ &= (-1)^k m(m-1)\cdots(m-k_{+}1) \\ &= (-1)^k m^{\underline{k}} \end{aligned}$$

where $m = -n + k - 1$. Use this to show then $n \leq -1$ that $m \geq k$ and so $k! | n^{\underline{k}} = (-1)^k m^{\underline{k}}$ in this case. This only leaves the cases $n = 0, 1, , \ldots, k-1$, which are not hard. □

The following is just a restatement of the last result.

Proposition 12. *For any positive integer k the product of k consecutive integers is divisible by $k!$.*

Proof. If we have a list of k consecutive integers and the largest one in the list is n, then the list is just $n, n-1, n-2, \ldots, (n-k+1)$ and the product of these is $n(n-1)(n-2)\cdots(n-k+1)$. So the result follows from Proposition 11. □

2. The division algorithm.

To start we recall how long division works, for example dividing 367 by 15 gives

$$\begin{array}{r@{\,}r} & 24 \\ 15\,\big) & \overline{367} \\ & \underline{30} \\ & 67 \\ & \underline{60} \\ & 7 \end{array}$$

and this tells us is that 15 goes into 367 24 times with a remainder of 7 left over. That is

$$\frac{367}{15} = 24 + \frac{7}{15}.$$

As this is a number theory class and we are mostly working with whole numbers multiply by 15 to clear of fractions to get

$$367 = 24 \cdot 15 + 7.$$

More generally if a and b are positive integers we can divide a into b, that is

$$\begin{array}{r} q \\ a\,\overline{)\,b} \\ \vdots \\ \hline r \end{array} \qquad \text{that is} \qquad \frac{b}{a} = q + \frac{r}{a}$$

to get a quotient, q, and remainder, r, which are related to the original integers a and b by

$$b = qa + r \qquad \text{and} \qquad 0 \leq r < a.$$

There is nothing special about a and b being positive. The next result does back to Euclid.

Theorem 13 (The division algorithm)**.** *Let a and b be integers with $a \neq 0$. Then there are unique integers q and r such that*

$$b = qa + r \qquad \textit{and} \qquad 0 \leq r < |a|.$$

The number q is the ***quotient*** *and r is the* ***remainder****.*

Saying that q and r are unique, means that if q' and r' and q and r are integers with

$$b = q'a + r' = qa + r \qquad \text{and} \qquad 0 \leq r' < |a| \quad \text{and} \quad 0 \leq r \leq |a|$$

then $q' = q$ and $r' = r$.

Proof of the division algorithm: Let S be the set of nonnegative integers of the form $b - ka$ where k is an integer. That is

$$S = \{b - ka : k \in \mathbb{Z} \text{ and } b - ka \geq 0\}.$$

Then S is non-empty. So see this we consider two cases.

Case1: $b \geq 0$. Let $k = 0$ to get that $b = b - 0a \in S$, which implies $S \neq \varnothing$.

Case 2: $b < 0$. Let $k = 2ba$. Then $b - ka = b - (2ba)a = (1 - 2a^2)b$. As $a \neq 0$ we have $a^2 > 0$ and as a^2 is an integer, this implies $a^2 \geq 1$. But then $(1 - 2a^2) \leq (1 - 2) = -1$. Therefore $(1 - 2a^2)$ is negative. And we are assuming $b < 0$. Whence $b - ka = (1 - 2a^2)b$ is a product of negative numbers and thus is positive. Therefore $b - ka \in S$ and so $S \neq \varnothing$ in this case also.

Also S is bounded below, as each element of S is ≥ 0. Thus S is non-empty and bounded below. Whence, by the Well Ordering Principle, S has a smallest element. Call this element r. By the definition of S, there is an integer q with $r = b - qa$. We now show that $0 \leq r < a$. Assume, towards a contradiction, that this is not the case. Then $r \geq |a|$. Also $|a| = \pm a$, where the plus holds when $a > 0$ and the minus sign holds when $a < 0$. Then subtract $|a|$ from both sides of $r = b - qa$ to get

$$r - |a| = b - qa - |a| = b - qa - \pm a = b - (q \pm 1)a = b - ka$$

where $k = (q \pm 1)$ is an integer. We are assuming $r \geq |a|$. Thus $r - |a| \geq 0$. This shows that $r - |a| = b - ka \in S$. But $r - |a| < r$, that is $-|a|$ is smaller than a, which contradicts that r was the smallest element of S. This competes the proof of the existence of q and r.

To show uniqueness assume that we have a pair q' and r' that satisfy the conclusion of the Theorem and let q and r be as in the proof of existence. Then

$$qa + r = q'a + r' \qquad \text{and} \qquad 0 \leq r < |a| \quad , \quad 0 \leq r' < |a|$$

Multiply $0 \leq r' < |a|$ by -1 to get $-|a| < -r' \leq 0$ and add this to $0 \leq r < |a|$. The result is

$$-|a| = 0 - |a| < r - r' < |a| + 0 = |a|.$$

This implies

$$|r - r'| < |a|.$$

Now rearrange $qa + r = q'a + r'$ as

$$a(q' - q) = r - r'.$$

Therefore

$$|a||q - q'| = |r - r'| < |a|.$$

As $|a| > 0$ this implies $0 \leq |q - q'| < 1$. But $|q - q'|$ is an integer, so we have $|q - q'| = 0$. This implies $q = q'$. Using this in $qa + r = q'a + r'$ implies $r = r'$ which completes both the proof of uniqueness and of the theorem. □

Problem 10. For the following a and b find the quotient, q, and remainder, r, when dividing b by a.

(a) $a = 19$, $b = 274$
(b) $a = 10$, $b = 4692$
(c) $a = 10$, $b = -4692$. □

Problem 11. For the following just find the remainder when b is divided by a.

(a) $a = 3$, $b = 2$, $b = 2^2$, $b = 2^3$, $b = 2^4$, $b = 2^5$. Can you find a pattern? If so can you prove your conjecture.
(b) $a = 5$, $b = 2$, $b = 2^2$, $b = 2^3$, $b = 2^4$, $b = 2^5$, $b = 2^6$, $b = 2^7$. Can you find a pattern? Again if you can, then prove your conjecture. □

2.1. **Even and odd integers.** The division algorithm lets us make a precise definition of even and odd numbers. If $n \in \mathbb{Z}$, then we divide by 2 to get

$$n = 2q + r \qquad \text{and} \qquad 0 \le r < 2.$$

The condition $0 \le r < 2$ implies that either $r = 0$ or $r = 1$. Thus every integer is of exactly one of the two forms

$$n = 2q, \qquad \text{or} \qquad n = 2q + 1.$$

So we make the definition

Definition 14. An integer n is ***even*** iff $n = 2q$ for some q and it is odd iff $n = 2q + 1$ for some q. □

What the division algorithm insures is that any integer is either even or odd (which I admit is not even a little surprising).

Here are some basic properties of even and odd numbers which I would guess that most of you already know.

Proposition 15. *(a) The sum of two even numbers is even.*
(b) The sum to two odd numbers is even.
(c) The sum of an even and odd number is odd.
(d) The product of two odd numbers is odd.
(e) The product and even number and odd number is even.
(f) The product of two odd numbers is even, and in fact is divisible by 4*.*

Proof. We only prove (c) and (d). For (c), let x be even and y odd. Then there are integers k and ℓ with $x = 2k$ and $y = 2\ell + 1$. The sum is $x + y = 2k + 2\ell + 1 = 2(k + \ell) + 1 = 2q + 1$ where $q = k + \ell$ is an integer. Thus $x + y$ is odd.

For (d) let x and y be odd. Then there are integers k and ℓ with $x = 2k+1$ and $y = 2\ell + 1$. Then the product is

$$xy = (2k + 1)(2\ell + 1) = 4k\ell + 2k + 2\ell + 1 = 2(2k\ell_k + \ell) + 1 = 2q + 1$$

where $q = 2k\ell_k + \ell$ is an integer. Therefore xy is odd. □

Problem 12*.* Prove part (f) of the last proposition. □

Proposition 16. *The product of two consecutive integers is even.*

Problem 13*.* Prove this. *Hint:* There are several ways to do this. One is to use Proposition 10. Anther is to let the product be $n(n + 1)$ and consider two cases: n is even, and n is odd. □

2.2. **Proof by cases.** Some proofs naturally split into cases. As an example let n be an integer and divide it by 4 to get

$$n = 4q + r \qquad \text{with} \qquad 0 \le r < 4.$$

This the only possible remainders when an integer is divided by 4 are 0, 1, 2, and 3. Thus the even integers are either of the form $4k$ or $4k + 2$ and the odd numbers are all of the form $4k + 1$ and $4k + 3$. Showing the following gives an example of a proof by cases.

Proposition 17. *The sum of two consecutive odd numbers is divisible by 4. That is if n is odd, then $n + (n + 2)$ is divisible by 4.*

Proof. As n is odd it is either of the form $n = 4k + 1$ or $n = 4k + 3$.

Case 1: $n = 4k + 1$. Then

$$n + (n + 2) = 4k + 1 + (4k + 1 + 2) = 8k + 4 = 4(2k + 1)$$

which is divisible by 4.

Case 2: $n = 4k + 3$. Then

$$n + (n + 2) = 2k + 3 + (2k + 3 + 2) = 4k + 8 = 4(k + 2)$$

which is also divisible by 4.

So in all possible cases the sum is divisible by 4, which completes the proof. □

Problem 14. Show that the product of two consecutive even integers is divisible by 8. That is if n is even show that $8 \mid n(n + 2)$. *Hint:* Either $n = 4k$ or $n = 4k + 2$. □

Problem 15. Show that the difference of the squares of two consecutive odd integers is divisible by 8. That is a and b are consecutive odd integers, then $8 \mid (b^2 - a^2)$. *Hint:* The assumption that a and b are consecutive odd integers means that a is odd and $b = a + 1$. Consider the cases $a = 4k + 1$ and $a = 4k + 3$. □

Problem 16. If $n = k^2$ is the square of in integer, show the last digit of n is either 0, 1, 4, 5, 6, or 9. *Hint:* The important thing to realize is that if a positive integer is divided by 10, the remainder is just the last digit of the number. For example if $n = 396$, then $n = 10(39) + 6$ so the remainder is 6.

We can assume that $k > 0$. If we divide k by 10 the possible remainders (last digits) are $0, 1, 2, \ldots, 8, 9$, thus we have that k is of one of the ten following forms:

$$k = 10q, k = 10q + 1, k = 10q + 2, k = 10q + 3, k = 10q + 4,$$
$$k = 10q + 5, k = 10q + 6, k = 10q + 7, k = 10q + 8, k = 10q + 9$$

So the proof splits into ten cases. Here are a couple of them. If $k = 10k+2$, then

$$n = k^2 = (10k + 2)^2 = 100k^2 + 40k + 4 = 10(10k^2 + 4) + 4$$

and the last digit is 4. If $k = 10k + 7$, then

$$\begin{aligned} n = (10k + 7)^2 = 100k^2 + 140k + 49 &= 100k^2 + 140k + 40 + 9 \\ &= 10(10k^2 + 14k + 4) + 9 \end{aligned}$$

so the last digit is 9. □

The previous problem shows that if the last digit of a number is 2, 3, 7, or 8, then it is not a perfect square. So we see 18,752 is not a perfect square by just noting the last digit is 2.

The following will be important to us when we take about representing integers as sums of two squares.

Proposition 18. *If a positive integer is of the form $n = 4q + 3$, than n is not the sum of two squares. That is there are no integers x and y such that $n = x^2 + y^2$.*

Problem 17. Prove this. *Hint:* For the expression $x^2 + y^2$ consider four cases: x and y both even, x even and y odd, x odd and y even, and x and y both odd. To give an example if x is even and y off, then we have $x = 2k$ and $y = 2\ell + 1$ for some k and ℓ. Then

$$x^2 + y^2 = (2k)^2 + (2\ell + 1)^2 = 4k^2 + 4\ell^2 + 4\ell + 1 = 4(k^2 + \ell^2 + \ell) + 1$$

so $x^2 + y^2$ is of the form $4q + 1$ and thus not of the form $4q + 3$ and so $x^2 + y^2 \neq n$ in this case. □

2.3. The definition and very basic properties of primes.

Definition 19. An integer p is prime iff $p > 1$ and the only positive factors of p are p and itself. □

Note that while the only positive factors of 1 are 1, we exclude it from being prime. This simplifies the statement of most results involving primes (otherwise there would be lots of provisos like, for all primes other than 1.)

Definition 20. An integer $n > 1$ is ***composite*** iff it has a positive factor other than 1 and itself. □

That is n is composite if and only if $n = ab$ with $a > 1$ and $b > 1$. An integers $n > 1$ is either prime or composite. As examples of composite numbers we have

$$6 = 2 \cdot 3, \quad 12 = 3 \cdot 4, \quad 100 = 4 \cdot 25, \quad 65893 = 131 \cdot 503.$$

Note to show that n is not prime, that is it is composite, we do not have to find all factors of n, only one factor of n other than 1 and n. For we have $12 = 3 \cdot 4$, which shows that 3 and 4 are factors of 12. But we could have also written $12 = 2 \cdot 6$ to see that it is not prime.

Making lists of primes takes some work, which fortunately has already been done for us. The first 200 primes are

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199, 211, 223, 227, 229, 233, 239, 241, 251, 257, 263, 269, 271, 277, 281, 283, 293, 307, 311, 313, 317, 331, 337, 347, 349, 353, 359, 367, 373, 379, 383, 389, 397, 401, 409, 419, 421, 431, 433, 439, 443, 449, 457, 461, 463, 467, 479, 487, 491, 499, 503, 509, 521, 523, 541, 547, 557, 563, 569, 571, 577, 587, 593, 599, 601, 607, 613, 617, 619, 631, 641, 643, 647, 653, 659, 661, 673, 677, 683, 691, 701, 709, 719, 727, 733, 739, 743, 751, 757, 761, 769, 773, 787, 797, 809, 811, 821, 823, 827, 829, 839, 853, 857, 859, 863, 877, 881, 883, 887, 907, 911, 919, 929, 937, 941, 947, 953, 967, 971, 977, 983, 991, 997, 1009, 1013, 1019, 1021, 1031, 1033, 1039, 1049, 1051, 1061, 1063, 1069, 1087, 1091, 1093, 1097, 1103, 1109, 1117, 1123, 1129, 1151, 1153, 1163, 1171, 1181, 1187, 1193, 1201, 1213, 1217, 1223.

A natural question is if this list goes on forever. The answer is yes, as we now show.

Lemma 21. *Let $k_1, k_2, \ldots, k_m$ be integers with $k_j \geq 2$ for all j and N be the product of these with 1 added, that is*

$$N = (k_1 k_2 \cdots k_m) + 1$$

then none of the k_j's are factors of N.

Proof. To make the notation simple we assume that $j = 1$ (which we can do by just reordering the factors in the product $k_1 k_2 \cdots k_m$). Then

$$N = (k_1 k_2 \cdots k_m) + 1 = k_1 q + 1$$

where $q = k_2 k_m \cdots k_m$. Note $0 \leq 1 < k_1$. Thus when we divide k_1 into N the remainder is 1. But if k_1 were a factor of N, the remainder would be 0. Whence k_1 is not a factor. □

The following is the easy part of the "Fundamental Theorem of Arithmetic" which says that any integer $n > 1$ factors into primes in a unique way. Here we just show that it factors into primes and leave the proof of uniqueness to later.

Proposition 22. *Let $n \geq 2$ be an integer. Then n factors into a finite number of primes. (This includes the case where n is prime, which we just consider it a product of one prime. And repeats are allowed i.e. $72 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3$.) In particular n has at least one prime factor.*

Problem 18. Prove this. *Hint:* This is a good example of the use of complete induction. The base case is easy: 2 is a prime. For the induction hypothesis assume for all integers k with $2 \leq k \leq n$ that k is a product of a finite number of primes. Now consider $n + 1$. If $n + 1$ is is prime we are done. If it is not prime it factors as $(n + 1) = k_1 k_2$ where $1 < k_1 \leq n$ and

$1 < k_2 \leq n$. Now you should be able to use the induction hypothesis to complete the proof. □

Theorem 23. *There are infinitely many primes.*

Problem 19. Prove this. *Hint:* The standard proof, which goes back to Euclid, starts as follows. Towards a contradiction assume there are only finitely primes. Let $p_1, p_2, \ldots, p_m$ be a list of all of the the primes and set

$$N = p_1 p_2 \cdots p_m + 1.$$

Use the last lemma and proposition to show that N has at least one prime factor, p, and that this prime is not in the list $p_1, p_2, \ldots, p_n$ and explain why this gives a contradiction. □

We can say a little more. If n is an odd number, then either it is of the form $4k+1$ or of the form $4k+3$.

Proposition 24. *The following hold*

(a) The product of two integers of the form $4k+1$ is of the form $4k+1$.
(b) The product of two integers of the form $4k+3$ is of the form $4k+1$.
(c) The product of an integer of the form $4k+1$ and one of the form $4k+3$ is of the form $4k+3$.
(d) The product of any number of integers of the form $4k+1$ is of the form $4k+1$

Proof. To prove (a):

$$(4k+1)(4k'+1) = 16kk' + 4(k+k') + 1 = 4(4kk' + k + k') + 1 = 4k'' + 1$$

with $k'' = (4kk' + k + k')$ an integer.

To prove (b):

$$(4k+3)(4k'+3) = 16kk' + 12(k+k') + 9 = 4(4kk' + 3(k+k') + 2) + 1 = 4k'' + 1$$

with $k'' = (4kk' + 3(k+k') + 2)$ an integer.

To prove (c):

$$(4k+1)(4k'+3) = 16kk' + 12k + 4k' + 3 = 4(kk' + 3k + k') + 3 = 4k'' + 3$$

with $k'' = (kk' + 3k + k')$ and integer.

Finally (a) follows from (a) be an easy induction using on the number of factors. □

Theorem 25. *There are infinitely many primes of the form $4k+3$.*

Problem 20. Prove this. *Hint:* Assume, towards a contradiction that there are only finitely many such primes. Let $p_1, p_2, \ldots, p_n$ be a list of these primes and set

$$N = 4p_1 p_2 \cdots p_n + 3.$$

Then N is a product of primes, say $q_1, q_2, \ldots, q_m$. If all these primes are of the form $4k+1$, then N would be of the form $4k+1$, while it is clearly of the form $4k+3$. □

We can take this circle of ideas just a little farther. If n is divided by 6 the possible remainders are $0, 1, 2, 3, 4, 5$ and so all integers are of one of the forms

$$\begin{gathered} 6k = 2 \cdot 3k, \quad 6k+1, \quad 6k+2 = 2(3k+1), \\ 6k+3 = 3(2k+1), \quad 6k+4 = 2(3k+2), \quad 6k+5. \end{gathered}$$

From this we see that any odd prime the two forms $6k+1$ or $6k+5$.

Theorem 26. *There are infinitely many primes of the form* $6k+5$.

Problem 21. Prove this. *Hint:* Assume, towards a contradiction that there are only finitely many such primes. Let $p_1, p_2, \ldots, p_n$ be a list of these primes and set

$$N = 6p_1p_2\cdots p_n + 5.$$

Now prove an analog of part (d) of Proposition 24 and then argue as in the proof of Theorem 25. □

The last two proposition have a generalization:

Theorem 27 (Dirichlet's theorem on arithmetic progressions)**.** *If a and b are positive integers and such that the only common factors of a and b are ± 1, then there are infinitely primes of the form $a + nb$.* □

Unfortunately the proof of this result is beyond the scope of this course. There can be long breaks between primes.

Proposition 28. *For each $n \geq 1$ there are n consecutive integers $m, m+1, \ldots, m+n-1$ none of which are prime.*

Problem 22. Prove this. *Hint:* Here is a construction for $n = 5$. Let $m = 6! + 2$. Then the five consecutive numbers

$$\begin{aligned} 6!+2 &= 2(1\cdot 3\cdot 4\cdot 5\cdot 6+1) \\ 6!+3 &= 3(1\cdot 2\cdot 4\cdot 5\cdot 6+1) \\ 6!+4 &= 4(1\cdot 2\cdot 3\cdot 5\cdot 6+1) \\ 6!+5 &= 5(1\cdot 2\cdot 3\cdot 4\cdot 6+1) \\ 6!+6 &= 6(1\cdot 2\cdot 3\cdot 4\cdot 5+1) \end{aligned}$$

are all composite. □

The following are both interesting and is good review of the algebra we did the first week of class.

Proposition 29. *If $a > 1$ and $a^n + 1$ is prime, then a is even and $n = 2^m$ for some m.*

Problem 23. Prove this. *Hint:* As special cases note $5^n + 1$ is even and thus has a factor of 2. And 24 has the odd factor 3 and therefore we can factor as follows $a^{24} + 1 = (a^8)^3 + 1 = (a^8 + 1)(a^{16} - a^8 + 1)$. □

Proposition 30. *If $a > 1$ and $a^n - 1$ is prime, then $a = 2$ and n is prime.*

Problem 24. Prove this. □

Remark 31. It is possible to be more explicit about the number of primes less than an integer n. If we set

$$\pi(n) = \text{Number of primes } p \text{ with } 1 < p \leq n$$

then the ***Prime Number Theorem***, due to Jacques Hadamard and Charles Jean de la Vallée-Poussin who independently gave proofs in 1896, is that

$$\pi(n) \sim \frac{n}{\ln(n)}.$$

This notation means

$$\lim_{n \to \infty} \frac{\pi(n)}{\left(\dfrac{n}{\ln(n)}\right)} = 1.$$

This is one of the most celebrated theorems in mathematics. A consequence is that if p_n is the n-th prime number, then

$$p_n \sim n \ln(n).$$

Unfortunately we will not be able to give proofs of these results in this class.

On the other hand there is much that is still unknown about primes. Here is a list of some well known unsolved problems about prime numbers.

The Goldbach conjecture. Every even number is the sum of two primes. This conjecture was made by Goldbach in 1742. There is a weaker version, that every odd number greater than seven is the sum of three primes, that is true. The proof of this was completed in 2013 and is based on work of Ivan Matveevich Vinogradov (1937), who proved the result for sufficiently large odd numbers, and Harald Helfgott who completed the proof in (2013).

The twin prime conjecture. There are infinitely primes p such that both p and $p+2$ are prime. It is claimed that this goes back to Euclid and if so it is the one of the oldest unsolved problem in mathematics. The first twin prime pairs are $(3,5)$, $(5,7)$, $(11,13)$, $(17,19)$, $(29,31)$, $(41,43)$, $(59,61)$, $(71,73)$, $(101,103)$. In 2013 Yitang Zhang, of the University of New Hampshire, made progress by showing there is an even number m such that there are infinitely many primes p with p and $p+m$ both prime. Since then it has been shown that it is possible to choose m with $m \leq 246$.

Primes of the form n^2+1: It is unknown if there are infinitely many primes of the form n^2+1. This question appears to have first been raised by Edmund Landau in 1912. There are heuristic arguments that imply there are infinitely many primes of this form, but to date no one has been able to make them rigorous.

2.4. **Ideals.**

Definition 32. A non-empty subset I of the integers is an ***ideal*** if has the following two properties.
(a) If $x, y \in I$ then $x + y \in I$.
(b) If $x \in I$ and $k \in \mathbb{Z}$, then $kx \in \mathbb{Z}$. □

Informally I is an ideal if and only if it is closed under sums and multiplication by elements of $\mathbb{Z}$. One consequence of the definition is that if $x \in I$ and we let $k = 0$ in (b), then $0 = 0x \in I$. Therefore all ideals contain 0. Anther basic consequence of the definition is

Proposition 33. *If I is an ideal in $\mathbb{Z}$ and $x, y \in I$ then for any $m, n \in \mathbb{Z}$ we have $mx + ny \in I$. As a special case ($m = 1$, $n = -1$) this implies that $x - y \in I$. Thus ideals are closed under subtraction.*

Problem 25. Prove this. □

Here is the most basic examples of an ideal.

Proposition 34. *For any $a \in \mathbb{Z}$, let I_a be the set of all multiples of a, that is*

$$I_a = \{ma : m \in \mathbb{Z}\}.$$

*Then I_a is an ideal. It is called the **principle ideal** generated by a.*

Problem 26. Prove this. *Hint:* To see that I_a is closed under sums let $x, y \in I_a$. Then there are $m, n \in \mathbb{Z}$ such that $x = ma$ and $y = na$. Then you can factor an a out of $x + y$ to see that it is a multiple of a and therefore in I_a. To see that I_a is closed under multiplication by elements of $\mathbb{Z}$, let $x \in I_a$, and $k \in \mathbb{Z}$. Then $x = ma$ for some $m \in \mathbb{Z}$. Then it is easy to see that kx is a multiple of a. □

The extreme examples are when $a = 0$ in which case we get

$$I_0 = \{0\}.$$

This is the ***zero ideal***. The other extreme is $a = 1$. Then for any $m \in \mathbb{Z}$ we have that $ma = m1 = m$ and so $m \in I_1$. Whence

$$I_1 = \mathbb{Z}.$$

Proposition 35. *Let $a, b \in \mathbb{Z}$ with $I_a = I_b$. Then $b = \pm a$.*

Problem 27. Prove this. *Hint:* If $a = 0$, then $I_a = \{0\}$, which implies $b = 0$, so that $a = b$. So assume that $a \neq 0$. The fact that we will use is that if m, n are integers and $mn = 1$ then either $m = n = 1$, or $m = n = -1$ (you do not have to prove this). As $I_a = I_b$ we have that $b \in I_a$, so that b is a multiple of a, say $b = ma$. Likewise $a \in I_b$ so that $b = na$ for some n. Combine these to get $a = mna$ and rest is up to you. □

The following result, which is important, is that all ideals in $\mathbb{Z}$ are principle.

Theorem 36. *(All ideals are principle.) Let I be an ideal in $\mathbb{Z}$. Then there is an $a \in \mathbb{Z}$ such that*

$$I = I_a.$$

That is every ideal is just the set of all multiples of some fixed integer a.

Problem 28. Prove this along the following lines.

(a) If is the zero ideal, that is $I = \{0\}$, then $I = I_0$ and we are done. So for the rest of the proof we assume $I \neq \{0\}$.

(b) Show that I contains at least one positive element. *Hint:* There is at least one nonzero element $x \in I$. But if $x \in I$, then so is $-x$.

(c) Let P be the set of positive elements in I. Explain why P has a smallest element.

(d) Let a be the smallest element of P, which is then the smallest positive element of I. Then for any $x \in I$ use the division algorithm to divide a into x to get

$$x = qa + r \qquad \text{with} \qquad 0 \leq r < a.$$

Explain why qa, and therefore $r = x = qa$, are in I.

(e) Show $r = 0$. *Hint:* If $r \neq 0$ then $0 < r < a$, and $r \in I$. But a is the smallest positive element of I.

(f) Conclude that $x = qa$ is a multiple of a. But x was an arbitrary element of I and therefore all elements of I are multiples of a. □

Problem 29. Let $a, b \in \mathbb{Z}$ and set

$$I_{a,b} = \{ma + nb : m, n \in \mathbb{Z}\}.$$

(a) Prove $I_{a,b}$ is an ideal.

(b) Show if I is an ideal and $1 \in I$, then $I = \mathbb{Z}$.

(c) What is $I_{7,11}$? □