MATH 4400 problems.

1. Below, $a$, $b$, $c$, and $d$ stand for positive integers. For each of the following assertions, give a proof or a counterexample.

(a) If $a \mid bc$ and $a \nmid b$, then $a \mid c$,
(b) if $\gcd(a, b) = 1$ and $a$ and $b$ both divide $c$, then $ab$ divides $c$,
(c) if $a \mid bc$ and $\gcd(b, c) = 1$, then $a \mid b$ or $a \mid c$,
(d) the integers $a/\gcd(a, b)$ and $b$ are relatively prime,
(e) if $a \mid b$ and $c \mid d$, then $ac \mid bd$,
(f) if $a \mid b + c$, then $a \mid b$ or $a \mid c$,
(g) if $a^3 \mid b^3$, then $a \mid b$,
(h) if $a$ is the largest integer for which $a^2 \mid c$, and also $b^2 \mid c$, then $b \mid a$.

Solution. (a) is false; take $a = 6$, $b = 2$, and $c = 3$.
(b) is true. Indeed, since $a \mid c$, we can write $c = ak$ where $k \in \mathbb{Z}$. Since $b \mid c = ak$ and $\gcd(b, a) = 1$, the fundamental lemma gives that $b \mid k$, so that $k = bq$ for some $q \in \mathbb{Z}$. Hence, $c = a(bq) = (ab)q$, and so $ab \mid c$.
(c) is false; same counterexample as in (a).
(d) is false; if $a = 12$ and $b = 18$, then $a/\gcd(a, b) = 2$ is not coprime to 18.
(e) is true. Write $b = ak$ and $d = c\ell$, where $k, \ell \in \mathbb{Z}$. Then $bd = ac(k\ell)$, so $ac \mid bd$.
(f) is false; take $a = 2$, $b = c = 1$.
(g) is true. Indeed, suppose $a^3 \mid b^3$. Then $3v_p(a) = v_p(a^3) \leq v_p(b^3) = 3v_p(b)$ for all primes $p$. Thus, $v_p(a) \leq v_p(b)$ for all primes $p$, which implies that $a \mid b$.
(h) is true. Notice that for $d \in \mathbb{Z}^+$, all of the following are equivalent:

$$d^2 \mid c \iff v_p(d^2) \leq v_p(c) \text{ for all primes } p$$

$$\iff 2v_p(d) \leq v_p(c) \text{ for all primes } p$$

$$\iff v_p(d) \leq \left\lfloor \frac{1}{2}v_p(c) \right\rfloor \text{ for all primes } p.$$

To find the largest $a \in \mathbb{Z}^+$ for which $a^2 \mid c$, we choose the exponents $v_p(a)$ as large as possible to find that

$$a = \prod_p p^\left\lfloor \frac{1}{2}v_p(c) \right\rfloor.$$

If $b^2 \mid c$, then the above analysis shows that $v_p(b) \leq \left\lfloor \frac{1}{2}v_p(c) \right\rfloor = v_p(a)$ for all primes $p$. Hence, $b \mid a$. □

2. If $a$ and $b$ are relatively prime, prove that $\gcd(a + b, a^2 - ab + b^2) = 1$ or 3.

Proof. Let $d = \gcd(a + b, a^2 - ab + b^2)$. Since $d \mid a + b$ and $d \mid a^2 - ab + b^2$, we see that

$$d \mid (a^2 - ab + b^2)(1) - (a + b)(a - 2b) = (a^2 - ab + b^2) - (a^2 - ab - 2b^2) = 3b^2.$$
Similarly,
\[ d \mid (a^2 - ab + b^2)(1) - (a + b)(b - 2a) = 3a^2. \]
So \( d \) divides \( 3a^2 \) and \( 3b^2 \), and so \( d \mid \gcd(3a^2, 3b^2) = 3 \gcd(a^2, b^2). \)

We claim that \( \gcd(a^2, b^2) = 1 \). Indeed, if \( \gcd(a^2, b^2) > 1 \), then there is a prime \( p \) dividing \( a^2 \) and \( b^2 \). But if \( p \mid a^2 = a \cdot a \), then \( p \mid a \), by Euclid’s lemma. Similarly, if \( p \mid b^2 \), then \( p \mid b \). This contradicts that \( \gcd(a, b) = 1 \). Hence, \( \gcd(a^2, b^2) = 1 \). Then the result of the last paragraph becomes the statement that \( d \mid 3 \). Since the only positive divisors of 3 are 1 and 3, the result follows.

3. Prove that there are no positive integers \( n \) for which \( n(n+1) \) is a perfect square. Hint: First show that if the product of two relatively prime positive integers is a square, then both of the factors are themselves squares.

**Proof.** First we tackle the hint. Suppose that \( n \cdot m \) is a perfect square, where \( \gcd(n, m) = 1 \). Suppose for the sake of contradiction that (at least) one of \( n \) and \( m \) is not a square. Without loss of generality, say it is odd. (In particular, \( v_p(n) \geq 1 \), so that \( p \mid n \).) Since \( n \) and \( m \) are relatively prime, \( p \nmid m \). So \( v_p(n \cdot m) = v_p(n) + v_p(m) = v_p(n) \) is also odd. But then \( n \cdot m \) is not a perfect square.

The integers \( n \) and \( n+1 \) are relatively prime, since any common divisor \( d \) would divide \((n+1) - n = 1 \). So if \( n(n+1) \) is a square, then \( n = a^2 \) and \( n+1 = b^2 \) for some positive integers \( a \) and \( b \). Since \( n < n+1 \), we have \( a < b \), so that \( b \geq a + 1 \). But then
\[ 1 = (n + 1) - n = b^2 - a^2 = (b - a)(b + a) \geq 1 \cdot (b + a) \geq 2, \]
an absurdity.

4. A **Mersenne prime** is a prime number of the form \( 2^n - 1 \), where \( n \) is a positive integer. For example, \( 7 = 2^3 - 1 \) is a Mersenne prime. Prove that if \( 2^n - 1 \) is prime, then \( n \) itself is prime. (The converse is not true, as the example \( 2^{11} - 1 = 23 \cdot 89 \) illustrates.)

**Proof.** We start from the identity
\[ x^N - 1 = (x - 1)(x^{N-1} + x^{N-2} + \cdots + x + 1), \] (1)
valid for all real numbers \( x \) and any positive integer \( N \). (If you don’t believe this, just multiply it out!) Suppose for the sake of contradiction that \( 2^n - 1 \) is prime but \( n \) is composite, and say \( n = ab \) with \( a > 1 \) and \( b > 1 \). We take \( N = b \) and \( x = 2^a \) in the factorization (1) to find that
\[ 2^n - 1 = 2^{ab} - 1 = (2^a - 1)(2^{a(b-1)} + 2^{a(b-2)} + \cdots + 2^a + 1). \]
Since \( a, b > 1 \), both factors on the right are larger than 1, contradicting that \( 2^n - 1 \) is prime.

5. Suppose that \( d \) divides \( ab \), where \( a, b, d \) are positive integers. Show that \( d \) can be written in the form \( d = d_1d_2 \), where \( d_1, d_2 \) are positive integers, \( d_1 \) divides \( a \), and \( d_2 \) divides \( b \). Show that \( d_1 \) and \( d_2 \) are uniquely determined by these conditions if \( a \) and \( b \) are relatively prime.
Proof. Let \( d_1 = \gcd(d, a) \), and let \( d_2 = d / \gcd(d, a) \). We claim that \( d_1 \) and \( d_2 \) satisfy the given conditions. Obviously \( d_1, d_2 \in \mathbb{Z}^+ \), \( d = d_1d_2 \), and \( d_1 \mid a \). So the only condition left to check is that \( d_2 \mid b \).

Since \( d \mid ab \), we can write \( ab = dq \) for some \( q \in \mathbb{Z} \). Dividing both sides by \( \gcd(d, a) \) gives

\[
\frac{a}{\gcd(d, a)} b = \frac{d}{\gcd(d, a)} q, \quad \text{so that} \quad \frac{d}{\gcd(d, a)} \mid \frac{a}{\gcd(d, a)} b.
\]

But \( d / \gcd(d, a) \) and \( a / \gcd(d, a) \) are relatively prime, so by the fundamental lemma, \( \frac{d}{\gcd(d, a)} \) divides \( b \). But \( d / \gcd(d, a) \) is what we were calling \( d_2 \), so we are done.

It remains to show that if \( a \) and \( b \) are relatively prime, then \( d_1 \) and \( d_2 \) are uniquely determined. Suppose that \( d \) has two decompositions, say \( d = d_1d_2 \) and \( d = d_1'd_2' \), where both decompositions satisfy the given conditions. Then \( d_1 \mid d = d_1'd_2' \). Moreover, \( d_1 \) is relatively prime to \( d_2' \), since \( \gcd(d_1, d_2') \) is a common divisor of the relatively prime pair \( a \) and \( b \). So by the fundamental lemma, \( d_1 \mid d_1' \). A similar argument, with the roles of the \( d_i \) and \( d_i' \) reversed, shows that \( d_1' \mid d_1 \). Hence, \( d_1 = d_1' \). Since \( d_1d_2 = d_1'd_2' \), we now deduce that \( d_2 = d_2' \). \( \square \)

6. Prove that there are infinitely many primes of the form \( 6k - 1 \), where \( k \in \mathbb{Z}^+ \). Hint: Imitate Euclid’s proof of the infinitude of primes. For a similar argument, see p. 28 of your textbook.

Proof. We start with a lemma, namely that every prime \( p > 3 \) is of the form \( 6k - 1 \) or \( 6k + 1 \) with \( k \) a positive integer.

Let \( p > 3 \) be prime. By the division algorithm, we can write \( p = 6k + r \) where \( r \in \{0, 1, 2, 3, 4, 5\} \). Integers \( \equiv 0, 2 \) or \( 4 \) (mod 6) have 2 as a prime factor while integers \( \equiv 3 \) (mod 6) have 3 as a factor, and both are impossible for primes \( p > 3 \). So \( r = 1 \) or \( r = 5 \). If \( r = 1 \), then \( p = 6k + 1 \) is already in the desired form, while if \( r = 5 \), then \( p = 6k + 5 = 6(k + 1) - 1 \).

Now we can prove that there are infinitely many primes of the form \( 6k - 1 \). Let \( q_1, q_2, \ldots, q_\ell \) be any finite list of primes of the form \( 6k - 1 \). We find another prime \( q \) of the form \( 6k - 1 \) not on the list. Consider the integer

\[
P := 6q_1q_2 \cdots q_\ell - 1.
\]

Then 2, 3, and every one of the \( q_i \) divide \( P + 1 = 6q_1 \cdots q_\ell \), so do not divide \( P \). Not all of the primes dividing \( P \) can be of the form \( 6k + 1 \), otherwise \( P \) itself would have the form \( 6k + 1 \). So there must be at least one prime \( q \) dividing \( P \) that is of the form \( 6k - 1 \), and this \( q \) is not on our original list \( q_1, \ldots, q_\ell \). \( \square \)

7. A Pythagorean triple is an ordered triple \( (x, y, z) \) of positive integers with the property that \( x^2 + y^2 = z^2 \). For example, \( (7, 24, 25) \) is such a triple. Prove that if \( (x, y, z) \) is a Pythagorean triple, then \( 60 \mid xyz \).

Proof. Since \( 60 = 2^2 \cdot 3 \cdot 5 \), we see from the fundamental theorem of arithmetic that it suffices to show that each of \( 2^2 \), 3, and 5 divide \( xyz \).
First we prove $4 \mid xyz$. If at least two of $x, y,$ and $z$, are even, this is true. So we can assume at most one is even. If $x$ and $y$ are both odd, then $z^2 \equiv x^2 + y^2 \equiv 1 + 1 = 2 \pmod{4}$, but the only squares mod 4 are 0 and 1. So one of $x$ and $y$ must be even while the other is odd. Say (without loss of generality) that $x$ is even, $y$ is odd, and $z$ is odd. Since every odd square is 1 (mod 8), we get that

$$x^2 = z^2 - y^2 \equiv 1 - 1 = 0 \pmod{8},$$

so $8 \mid x^2$. But then $2^2$ must divide $x$. Indeed, $2v_2(x) = v_2(x^2) \geq v_2(8) = 3$, so $v_2(x) \geq 3/2$. Since $v_2(x)$ is an integer, $v_2(x) \geq 2$; that is, $2^2 \mid x$.

Next we show $3 \mid xyz$. In fact, we prove that $3 \mid x$ or $3 \mid y$. Indeed, since both $1^2$ and $2^2$ are 1 (mod 3), if 3 divides neither $x$ nor $y$, then $z^2 \equiv x^2 + y^2 \equiv 1 + 1 = 2 \pmod{3}$. But 2 is not a square modulo 3, so this is impossible.

Finally we show $5 \mid xyz$. If not, then each of $x^2, y^2,$ and $z^2$ is congruent to one of 1 or 4 modulo 5. However, there are no solutions to $A + B \equiv C \pmod{5}$ with all of $A, B, C \in \{1, 4\}$. Indeed, mod 5, we have $1+1 \equiv 2, 1+4 \equiv 4+1 \equiv 0,$ and $4+4 \equiv 3$.  


MATH 6400 problems. Students in MATH 6400 must turn in (at least) two of these problems, in addition to the problems assigned for MATH 4400.

G1. Let $F(x)$ be a nonconstant polynomial with integer coefficients. Let $\mathcal{P}(F)$ be the set of primes which divide $F(n)$ for some integer $n$. For example, if $F(x) = x$, then $\mathcal{P}(F)$ is the entire set of primes, while if $F(x) = 2x - 1$, then $\mathcal{P}(F)$ consists just of the odd primes. Prove that $\mathcal{P}(F)$ is always an infinite set. Hint: Imitate Euclid’s proof of the infinitude of primes.

Proof. With $d$ denoting the degree of $F$ (so that $d \geq 1$ by hypothesis), write

$$F(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_d x^d.$$ 

If $a_0 = 0$, then every prime divides $F(0) = 0$, and we are done (by Euclid’s theorem). So we suppose in what follows that $a_0 \neq 0$. Note that for every $x$, we have

$$F(a_0 x) = a_0 + a_1 a_0 x + a_2 a_0^2 x^2 + \cdots + a_d a_0^d x^d$$

$$= a_0 G(x), \quad \text{where we set} \quad G(x) = 1 + a_1 x + a_2 x^2 + \cdots + a_d a_0^{n-1} x^d.$$ 

Thus, whenever $p \mid G(n)$ for $n \in \mathbb{Z}$, we have that $p \mid a_0 G(n) = F(n)$. So every prime dividing a value of $G$ belongs to $\mathcal{P}(F)$.

Suppose that $q_1, \ldots, q_k$ is any finite list of primes belonging to $\mathcal{P}(F)$. We show how to find a prime $q \in \mathcal{P}(F)$ not equal to any of the $q_i$. Choose an integer $n$ for which

$$G(n q_1 \cdots q_k) \notin \{-1, 1\}.$$ 

This is easy to do: By the fundamental theorem of algebra, we can have $G(n q_1 \cdots q_k) \in \{-1, 1\}$ for at most $2d$ values of $n$, so we simply choose an integer $n$ avoiding these. Then $G(n q_1 \cdots q_k)$ has some prime divisor $q$. As noted above, $q \in \mathcal{P}(F)$. Moreover, $q$ cannot be any of the $q_i$, since each

$$q_i \mid a_1 (n q_1 \cdots q_k) + a_2 a_0 (n q_1 \cdots q_k)^2 + \cdots + a_d a_0^{n-1} (n q_1 \cdots q_k)^d = G(n q_1 \cdots q_k) - 1. \quad \Box$$

G2. A positive integer $n$ is called multiplicatively perfect if $n$ is the product of all its proper divisors; in other words,

$$n = \prod_{d|n} d.$$ 

For example, 8 is multiplicatively perfect, since $8 = 1 \cdot 2 \cdot 4$. Classify all multiplicatively perfect numbers in terms of their prime factorizations.

Proof. We first evaluate $\prod_{d|n} d$ for a general $n \in \mathbb{Z}^+$. Note that the product, as we have written it, includes $n$ itself.

Whenever $d$ divides $n$, we can write $n = d \cdot (n/d)$, so that $n/d$ also divides $n$. Thus, every divisor $d$ has a conjugate divisor $n/d$. We now pair each divisor $d$ with its conjugate divisor $n/d$. Letting $\tau(n)$ denote the number of divisors of $n$, there are now two possibilities:
• If \( n \) is not a perfect square, then no \( d \) pairs with itself, and there are \( \tau(n)/2 \) pairs \( \{d, n/d\} \).

• If \( n \) is a perfect square, then \( n = m^2 \) for some \( m \in \mathbb{Z}^+ \). Excluding \( m \) from the list of divisors of \( n \) and pairing everything else off, we get \( (\tau(n) - 1)/2 \) pairs of conjugate divisors \( \{d, n/d\} \).

Multiplying the divisors in these conjugate pairs, we find that

\[
\prod_{d|n} d = n^{\tau(n)/2}.
\]

(When checking this, it is helpful to remember in the case when \( n = m^2 \) that \( m = n^{1/2} \).)

If we now exclude \( n \) from the product, then we find that

\[
\prod_{d|n, d<n} d = n^{\tau(n)/2 - 1}.
\]

Now \( n \) is multiplicatively perfect precisely when the right-hand side of this equation is \( n \), which occurs if and only if \( n = 1 \) or \( \tau(n) = 4 \).

So to finish this off, we need to characterize those numbers \( n \) have exactly 4 divisors. We take cases, depending on the number of primes dividing \( n \).

If \( n \) is a power of a single prime, say \( n = p^e \), then the divisors of \( n \) are \( 1, p, p^2, \ldots, p^e \), so there are a total of \( e + 1 \) divisors. So in order to have \( 4 \) divisors, it is necessary and sufficient that \( e = 3 \). So our first family of multiplicatively perfect numbers are the numbers \( p^3 \), with \( p \) prime.

Suppose next that \( n \) has exactly two prime divisors, say \( p_1 \) and \( p_2 \). Then already \( n \) is divisible by \( 1, p_1, p_2, \) and \( p_1p_2 \). So if \( n \) is to have four divisors, those must be all of the divisors of \( n \), which means that \( n = p_1p_2 \). So we obtain another class of multiplicatively perfect numbers, namely \( p_1p_2 \) for distinct primes \( p_1 \) and \( p_2 \).

Finally, if \( n \) has more than two prime divisors, say \( p_1, p_2, \) and \( p_3 \), then \( n \) has more than \( 4 \) divisors (e.g., \( 1, p_1, p_2, p_3, p_1p_2 \) is already more than four), and so we get no new examples this way.

So the multiplicatively perfect numbers include \( 1 \) (the degenerate example), \( p^3 \) for \( p \) prime, and \( p_1p_2 \) for primes \( p_1 \neq p_2 \).

G3. Let \( a \) be an integer with \( a > 1 \). Prove that if \( n, m \in \mathbb{Z}^+ \), then \( \gcd(a^n - 1, a^m - 1) = a^{\gcd(n, m)} - 1 \).

**Proof.** Suppose \( n > m \), and write \( n = mq_1 + r_1 \), where \( 0 \leq r_1 < m \). We first show that in this case,

\[
\gcd(a^n - 1, a^m - 1) = \gcd(a^m - 1, a^{r_1} - 1).
\]

(2)

If this is proved, then we write \( m = r_1q_2 + r_2 \) with \( 0 \leq r_2 < r_1 \). We then get the same equality of gcds but with \( (m, r_1) \) replaced by the pair \( (r_1, r_2) \). We can continue the process; the pairs we obtain are the same pairs that showed up in our earlier discussion of the Euclidean algorithm. In particular, we eventually reach the pair \( (r_{n-1}, 0) \), where
$r_{n-1} = \gcd(n, m)$ is the last nonzero remainder in the Euclidean algorithm. So we will find that
\[
gcd(a^n - 1, a^m - 1) = \gcd(a^{\gcd(n,m)} - 1, a^0 - 1) = \gcd(a^{\gcd(n,m)} - 1, 0) = a^{\gcd(n,m)} - 1,
\]
as desired.

It remains to prove the initial claim (2). For this, it is enough to show that the set $S_1$ of common divisors of $a^n - 1$ and $a^m - 1$ coincides with the set $S_2$ of common divisors of $a^m - 1$ and $a^{r^1} - 1$. Say $d \in S_1$. Then $a^m \equiv 1 \pmod{d}$. Since $a^n \equiv 1 \pmod{d}$, we can thus write
\[
0 \equiv a^n - 1 = (a^m)^q a^r - 1 \equiv 1^q \cdot a^r - 1 \equiv a^r - 1 \pmod{d}.
\]
Hence, $d \mid a^r - 1$. So $d \in S_2$. On the other hand, if $d \in S_2$, then $a^m \equiv 1 \pmod{d}$ and $a^r \equiv 1 \pmod{d}$, so that
\[
a^n - 1 = (a^m)^q a^r - 1 \equiv 1^q \cdot 1 - 1 \equiv 0 \pmod{d},
\]
and so $d \mid a^n - 1$; hence $d \in S_1$. So $S_1 = S_2$. \qed

G4. A positive integer $n$ is called powerful if every prime that appears in its prime factorization occurs to the second power or higher. For example, all squares are powerful numbers, as is $392 = 2^3 \cdot 7^2$. Show that every powerful number can be written as the product of a square and a cube. Using this, prove that for every real number $x > 0$, the number of powerful numbers not exceeding $x$ is at most $3x^{1/2}$.

Proof. Every powerful number can be written in the form $p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$, where $p_1 < p_2 < \cdots < p_k$ are distinct primes, and each exponent $e_i \geq 2$. Now the product of squares is a square, and the product of cubes is a cube. So it is enough to show that each of the individual prime powers $p_i^{e_i}$ appearing in our factorization can be written as the product of a square and a cube.

So let $p^e$ be a prime power, where $e \geq 2$. Write $e = 3k + r$, where $r \in \{0, 1, 2\}$. If $r = 0$, then $p^e = 1^2 \cdot (p^{e/3})^3$ is a representation of $p^e$ in the desired form. If $r = 2$, then we can write $p^e = p^2 \cdot (p^{e/3})^3$. Finally, suppose $r = 1$. Since $e \geq 2$, we have $k \geq 1$. Hence, $p^e = (p^2)^2(p^{k-1})^3$ is a representation of the desired form.

It remains to prove the upper bound of $3x^{1/2}$ on the number of powerful numbers in $[1, x]$. If $n \leq x$ is powerful, write $n = a^2 b^3$. We see that the number of powerful $n \leq x$ is at most the number of ordered pairs $(a, b) \in \mathbb{Z}^+ \times \mathbb{Z}^+$ with $a^2 b^3 \leq x$. So for a fixed value of $b$, the number of possible $a$ is at most $x/b^3$. Now we sum over $b$ to get an upper bound of $x \sum_{b \geq 1} \frac{1}{b^{3/2}}$. Finally, by the integral test,
\[
\sum_{b \geq 1} \frac{1}{b^{3/2}} \leq 1 + \int_1^\infty \frac{dt}{t^{3/2}} = 3. \qed
\]