1. Find the following:

(a) The gcd and lcm of 288 and 600.

- From the Euclidean algorithm we find \( \gcd(288, 600) = 24 \). Then \( \text{lcm}(288, 600) = \frac{288 \cdot 600}{24} = 7200 \).

(b) The gcd and lcm of \( 2^83^11^57^38^112^2 \) and \( 2^43^85^77^311_{11}^2 \).

- From the prime factorizations, the gcd is \( 2^43^85^77^11_{11}^1 \) and the lcm is \( 2^83^11^57^38^112^1 \).

(c) The total number of positive integers that divide \( 2^23^45^77^3 \). [Hint: Consider possible prime factorizations.]

- Such a divisor is of the form \( 2^a3^b5^c7^d \) where \( a \in \{0, 1, 2\} \), \( b \in \{0, 1, 2, 3, 4\} \), \( c \in \{0, 1, \ldots, 9\} \), and \( d \in \{0, 1, 2, 3\} \).
- Therefore there are \( 3 \cdot 5 \cdot 10 \cdot 4 = 600 \) total divisors.

(d) A positive integer \( n \) such that \( n/2 \) is a perfect square and \( n/3 \) is a perfect cube.

- If \( n = 2^a3^b \) then we want \( 2^{-1}3^b \) to be a square, so both exponents are even, and \( 2^a3^{b-1} \) to be a cube, so both exponents are multiples of 3.
- Testing small possibilities shows that \( a = 3, b = 4 \) satisfies all the requirements, so \( n = 2^33^4 = 648 \) works. (In fact, it is the smallest example.)

(e) A triple of positive integers \( (a, b, c) \) such that \( \gcd(a, b), \gcd(a, c), \) and \( \gcd(b, c) \) are all greater than 1, but the only common divisors of all three of \( a, b, c \) are \( \pm 1 \).

- The idea is that we can use a different prime for each pairwise gcd, and then no prime will divide all three of the integers.
- So if we try \( \gcd(a, b) = 2 \), \( \gcd(a, c) = 3 \), and \( \gcd(b, c) = 5 \), we see that \( a \) is a multiple of 6, \( b \) is a multiple of 10, and \( c \) is a multiple of 15. Indeed, \( (a, b, c) = (6, 10, 15) \) has the desired property.
  (There are many others, of course.)

(f) The elements \( 1 + 2\sqrt{5}, 9 + 4\sqrt{5}, 5 + \sqrt{5}, \) and \( 2 - \sqrt{5} \) that are units in the ring \( \mathbb{Z}[\sqrt{5}] \). For the elements that are units, also find their multiplicative inverses.

- We use the norm map \( N(a + b\sqrt{5}) = a^2 - 5b^2 \) and the fact that an element is a unit if and only if its norm is \( \pm 1 \).
- Since \( N(1 + 2\sqrt{5}) = 1^2 - 5 \cdot 2^2 = -19 \), we see \( 1 + 2\sqrt{5} \) is not a unit.
- Since \( N(9 + 4\sqrt{5}) = 9^2 - 5 \cdot 4^2 = 1 \), we see \( 9 + 4\sqrt{5} \) is a unit. The norm map calculation says \( (9 + 4\sqrt{5})(9 - 4\sqrt{5}) = 1 \), so the multiplicative inverse is \( 9 - 4\sqrt{5} \).
- Since \( N(5 + \sqrt{5}) = 5^2 - 5 \cdot 1^2 = 20 \), we see \( 5 + \sqrt{5} \) is not a unit.
- Since \( N(2 - \sqrt{5}) = 2^2 - 5 \cdot 1^2 = -1 \), we see \( 2 - \sqrt{5} \) is a unit. The norm map calculation says \( (2 - \sqrt{5})(2 + \sqrt{5}) = -1 \), so the multiplicative inverse is \( -2 - \sqrt{5} \).

(g) The values of \( 6 + 13, 6 - 13, \) and \( 6 \cdot 13 \) in \( \mathbb{Z}/11\mathbb{Z} \). Write your answers as \( \bar{a} \) where \( 0 \leq a \leq 10 \).

- We have \( 6 + 13 = 19 = \bar{8}, 6 - 13 = -7 = \bar{4}, \) and \( 6 \cdot 13 = 78 = \bar{1} \).

(h) All integers \( n \) with the property that \( \pi + 7 = \overline{1} \) modulo 23. [Hint: The answer is not “\( n = 17 \)”]

- The solution is \( \overline{1} - 7 = -6 = \bar{17} \). This means \( n \equiv 17 \pmod{23} \), so the solutions are \( n = 17 + 23k \) for an arbitrary integer \( k \).
2. If $R$ is a commutative ring with 1, we say an element $r \in R$ is irreducible if $r$ is not a unit and there exists no “factorization” $r = ab$ where neither $a$ nor $b$ is a unit.

**Example:** In $R = \mathbb{Z}$, the irreducible elements are prime numbers (and their negatives).

**Example:** In $R = \mathbb{Z}[i]$, the element $3 - i$ is not irreducible, because $3 - i = (1 - i)(2 + i)$ and neither $1 - i$ nor $2 + i$ is a unit.

**Example:** In $R = \mathbb{Z}[\sqrt{2}]$, the element $\sqrt{2}$ is irreducible, because if $\sqrt{2} = ab$ then $2 = N(\sqrt{2}) = N(a)N(b)$ and then one of $N(a), N(b)$, and hence one of $a, b$, would have to be a unit. More generally, if an element has prime norm in $\mathbb{Z}[\sqrt{D}]$, then it is always irreducible (but note that there can also exist irreducible elements of non-prime norm).

(a) Inside the ring $R = 2\mathbb{Z}$ of even integers, identify which of the elements 2, 4, 6, 8, 10, and 30 are irreducible.

- We cannot write 2, 6, 10, or 30 as the product of two even numbers (since such a product is always divisible by 4), so these elements are **irreducible**.
- On the other hand, 4 = $2 \cdot 2$ and 8 = $2 \cdot 4$ can be factored, so they are **not irreducible**.

(b) Inside the ring $R = 2\mathbb{Z}$ of even integers, show that 60 has two different irreducible factorizations as products of positive numbers.

- From (a) we know that 2, 6, 10, and 30 are all irreducible, and so we have the two factorizations $60 = 2 \cdot 30 = 6 \cdot 10$.

(c) Inside the ring $R = \mathbb{Z}[i]$, identify which of the elements $1+i$, $2+i$, $3+i$, and $4+i$ are irreducible.

- We compute the norms of these elements: $N(1+i) = 2$, $N(2+i) = 5$, $N(3+i) = 10$, and $N(4+i) = 17$.
- Since 2, 5, and 17 are prime, using the reasoning from the third example above, then the corresponding elements $1+i$, $2+i$, and $4+i$ are **irreducible**.
- On the other hand, using a similar calculation to the second example above, we can see that $3+i = (1+i)(2-i)$ so it is **not irreducible**.

3. Draw the addition and multiplication tables modulo 7. (For ease of writing, you may omit the bars in the residue class notation.) Then, for each residue class, identify whether it is a unit, and if so, calculate its multiplicative inverse.

- Here are the addition and multiplication tables for $\mathbb{Z}/7\mathbb{Z}$:

<table>
<thead>
<tr>
<th>+</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>6</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>6</td>
<td>6</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>.</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>2</td>
<td>4</td>
<td>6</td>
<td>1</td>
<td>3</td>
<td>5</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>3</td>
<td>6</td>
<td>2</td>
<td>5</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>4</td>
<td>1</td>
<td>5</td>
<td>2</td>
<td>6</td>
<td>3</td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td>5</td>
<td>3</td>
<td>1</td>
<td>6</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>6</td>
<td>0</td>
<td>6</td>
<td>5</td>
<td>4</td>
<td>3</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>

- Every nonzero residue class is invertible: $1^{-1} = 1$, $2^{-1} = 4$, $3^{-1} = 5$, $4^{-1} = 2$, $5^{-1} = 3$, and $6^{-1} = 6$. 

---

2
4. Let $n$ be a positive integer greater than 1.

(a) Show that if $n$ is composite, then $n$ must have at least one divisor $d$ with $d \leq \sqrt{n}$. Deduce that if $n$ is composite, then $n$ has at least one prime divisor $p \leq \sqrt{n}$.

- Since $n$ is composite, we can write $n = ab$ for some $1 < a < b < n$.
- Then we see that $a^2 \leq ab = n$, and so $a \leq \sqrt{n}$. Thus, $n$ has a divisor that is $\leq \sqrt{n}$ as claimed.
- For the second statement, simply let $p$ be any prime divisor of $a$: then $1 < p \leq a \leq \sqrt{n}$, and $p$ divides $a$ hence $n$. Thus, $n$ has a prime divisor $\leq \sqrt{n}$.

(b) Show that if no prime less than or equal to $\sqrt{n}$ divides $n$, then $n$ is prime.

- This is simply the contrapositive of the second statement in part (a): if $n$ has no prime divisor $p \leq \sqrt{n}$ then $n$ is not composite (i.e., $n$ is prime).

(c) Use part (b) to explain why the representation $89 = 2 \cdot 5 \cdot 11 - 3 \cdot 7$ shows that $89$ is prime.

- The point is that since $2, 3, 5, 7, 11$ are all prime, none of them can divide the right-hand side, since each of them appears in one term but not the other. Since $\sqrt{89} < 10$, and the primes less than 10 are $2, 3, 5, 7, 11$, part (a) implies that $89$ is prime.

5. Let $R$ be a commutative ring with 1 and let $r$ be an element of $R$.

(a) Show that if $r$ is a unit then $-r$ and $r^{-1}$ are also units.

- Suppose $r$ is a unit with inverse $r^{-1}$.
- Then $(-r)(-r^{-1}) = (-1)^2rr^{-1} = 1 \cdot 1 = 1$, so $-r^{-1}$ is a multiplicative inverse for $-r$ and thus $-r$ is a unit.
- Likewise, since $r \cdot r^{-1} = 1$, this means that $r$ is a multiplicative inverse for $r^{-1}$, so $r^{-1}$ is also a unit.

(b) Show that if $r$ and $s$ are units, then $rs$ is also a unit.

- Suppose $r$ and $s$ are units with respective inverses $r^{-1}$ and $s^{-1}$.
- Then $rs(s^{-1}r^{-1}) = r(s(s^{-1})r^{-1}) = r1r^{-1} = rr^{-1} = 1$. So $s^{-1}r^{-1}$ is a multiplicative inverse for $rs$, meaning $rs$ is a unit.

6. Suppose $a, b, c, m$ are integers and $m > 0$. Prove the following basic properties of modular congruences (these properties are mentioned but not proven in the notes; you are expected to give the details of the proofs):

(a) For any $a$, $a \equiv a \pmod{m}$.

- Since $m \mid 0$, we have $m \mid (a - a)$, so by definition of modular congruence, $a \equiv a \pmod{m}$.

(b) If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$.

- Suppose $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$. Then by definition, $m \mid (b - a)$ and $m \mid (c - b)$.
- Therefore $m$ also divides $(c - b) + (b - a) = c - a$, so by definition, $a \equiv c \pmod{m}$.

(c) If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a + c \equiv b + d \pmod{m}$.

- Suppose $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$. Then by definition, $m \mid (b - a)$ and $m \mid (d - c)$.
- Therefore $m$ also divides $(d - c) + (b - a) = (b + d) - (a + c)$, so by definition, $a + c \equiv b + d \pmod{m}$.

(d) If $a \equiv b \pmod{m}$, then $ac \equiv bc \pmod{mc}$ for any $c > 0$.

- Suppose $a \equiv b \pmod{m}$. Then by definition, $m \mid (b - a)$. So by properties of divisibility, we see that $mc$ divides $(b - a)c = bc - ac$.
- So by definition, this means $ac \equiv bc \pmod{mc}$ as claimed. (Note that $c > 0$ is needed only because the modulus $mc$ is required to be positive.)
7. The goal of this problem is to analyze the maximum possible number of divisions that the Euclidean algorithm requires (in the parlance of computer science, this represents the worst-case time complexity). One might expect the slowest possible computation to occur when all of the quotients in the division algorithm are as small as possible, and the resulting gcd is also 1; our goal is to prove this fact.

(a) As motivation, find \(a\) and \(b\) such that the Euclidean algorithm takes 6 divisions to compute their gcd of 1, and all of the corresponding quotients except the last are 1. In other words, find \(a\) and \(b\) such that
\[
\begin{align*}
    a &= q_1b + r_1 \\
    b &= q_2r_1 + r_2 \\
    r_1 &= q_3r_2 + r_3 \\
    r_2 &= q_4r_3 + r_4 \\
    r_3 &= q_5r_4 + r_5 \\
    r_4 &= q_6r_5
\end{align*}
\]
where \(q_1 = q_2 = q_3 = q_4 = q_5 = 1, q_6 = 2,\) and \(r_5 = 1.\) (Note that the last two quotients cannot be 1 if the last remainder is also 1.)

- Solving from the bottom up, we see \(r_4 = 2, r_3 = 2 + 1 = 3, r_2 = 3 + 2 = 5, r_1 = 5 + 3 = 8, b = 8 + 5 = 13,\) and \(a = 13 + 8 = 21.\)
- Thus, \(a = [21]\) and \(b = [13]\) (Notice the presence of the Fibonacci numbers here!)

(b) Prove that the Euclidean algorithm requires exactly \(n\) divisions to compute \(\gcd(F_{n+2}, F_{n+1})\), where \(F_n\) is the \(n\)th Fibonacci number as defined on homework 1.

- We prove the result by induction on \(n\).
- The base case \(n = 1\) follows from observing that \(F_2 = 1\) divides \(F_3 = 2.\)
- For the inductive step, suppose that \(n \geq 2\) and that the Euclidean algorithm requires \(n\) divisions to compute \(\gcd(F_{n+2}, F_{n+1}).\)
- Then we have \(F_{n+3} = 1 \cdot F_{n+2} + F_{n+1},\) so the remainder upon dividing \(F_{n+3}\) by \(F_{n+2}\) is \(F_{n+1}\) (since \(F_{n+1} < F_{n+2}\)).
- Hence by the inductive hypothesis, since it takes \(n\) divisions to compute \(\gcd(F_{n+2}, F_{n+1})\), it will take \(n + 1\) divisions to compute \(\gcd(F_{n+3}, F_{n+2}),\) as claimed.

(c) Suppose that \(b \leq a\) and that \(a\) and \(b\) are integers for which the Euclidean algorithm requires at least \(n \geq 2\) divisions to compute \(\gcd(a, b).\) Prove that \(b \geq F_{n+1}\) and \(a \geq F_{n+2}.

- We prove the result by induction on \(n\).
- The base case \(n = 2\) is the case where \(a = q_1b + r_1\) and \(b = q_2r_1,\) where \(r_1\) is positive. In such a case, we see that \(b \geq 1\) and \(a \geq 1 + 1 = 2,\) so indeed \(b \geq F_2\) and \(a \geq F_3\) as claimed.
- For the inductive step, suppose \(b \leq a\) and the Euclidean algorithm for computing \(\gcd(a, b)\) requires \(n + 1\) divisions.
- If we take \(a = q_1b + r_1,\) then by assumption, applying the Euclidean algorithm to compute \(\gcd(b, r_1)\) requires \(n\) divisions. Hence by the inductive hypothesis, we have \(b \geq F_{n+2}\) and \(r_1 \geq F_{n+1}.\)
- Then \(a = q_1b + r_1 \geq b + r_1 \geq F_{n+2} + F_{n+1} = F_{n+3}\), and so \(b \geq F_{n+2}\) and \(a \geq F_{n+3}\) as required.

(d) Deduce that if \(b \leq a\) and \(a, b\) are the smallest integers for which the Euclidean algorithm requires exactly \(n\) divisions, then \(a = F_{n+2}\) and \(b = F_{n+1}.

- This follows immediately from parts (b) and (c): (b) shows that \((F_{n+2}, F_{n+1})\) does require \(n\) divisions, while (c) shows that any other pair requiring at least \(n\) divisions has \(a\) and \(b\) at least as large.

- **Remark:** As shown on homework 1, the Fibonacci numbers grow exponentially: \(F_n \approx \frac{1}{\sqrt{5}} \phi^n.\) Because \(\log_\phi(b\sqrt{5}) - 2 < 5\log_{10}(b)\), part (d) implies that the Euclidean algorithm will compute \(\gcd(a, b)\) with a number of divisions that is at most 5 times the number of base-10 digits of \(b\). Thus for example, using the Euclidean algorithm to compute the gcd of two 1000-digit numbers will only take at most 5000 steps (which is very efficient!).