1. Problems that can be done up to Wed 9

Some congruence notation has been used, but the problems can be solved without congruences.

Exercise 1.1. See lecture notes.

Exercise 1.2. See lecture notes.

Exercise 1.3. True or false.
   a) False. For example \((2, 3) = 1\) but \((3 \cdot 2 + 1, 3) = (9, 3) = 3\).
   b) False. Consider the consecutive primes 5, 7 and 11, we then have that \(2 \times 5 \times 7 \times 11 + 1\) is divisible 3.
   c) True. 3 is a prime.
   d) True. If \(x \equiv 0 \pmod{3}\), then \(2x^3 + x^2 + 2 \equiv 2 \not\equiv 0 \pmod{3}\). If \(x \equiv 1 \pmod{3}\), then \(2x^3 + x^2 + 2 \equiv 2 \not\equiv 0 \pmod{3}\).

Exercise 1.4. We have

\[
\begin{align*}
587 &= 345 + 242, \\
345 &= 242 + 103, \\
242 &= 103 \times 2 + 36, \\
103 &= 36 \times 2 + 31, \\
36 &= 31 + 5, \\
31 &= 5 \times 6 + 1, \\
5 &= 5 \times 1 + 0.
\end{align*}
\]

Hence the gcd is \((587, 345) = 1\). Now use

\[
[587, 345] = \frac{587 \times 345}{(587, 345)} = \frac{202515}{1} = 202515.
\]

Exercise 1.5. One way to do this is to use the Euclidean algorithm. We have

\[
\begin{align*}
n^3 - 1 &= n(n^2 - 1) + (n - 1), \\
n &= (n - 1) + 1, \\
n - 1 &= 1 \times (n - 1) + 0.
\end{align*}
\]

(1.1)

So the gcd is \((n, n^3 - 1) = 1\), if \(n \geq 1\).

Exercise 1.6. Since every number has a unique prime factorization (by the FTA), the set of positive divisors of \(n\) is

\[
S = \{p_1^a p_2^b p_3^c | 0 \leq a \leq 5, 0 \leq b \leq 1, 0 \leq c \leq 4\}.
\]

The number of elements in this set is \(6 \times 2 \times 5 = 60\), i.e. \(|S| = 60\). This is the number of positive divisors of \(n\).
Exercise 1.7. Yes. If \( n = 3 \), then these are 3, 5, 17. However, if \( n > 3 \), then these will never all be simultaneously prime. If \( n > 3 \) and \( n \equiv 0 \pmod{3} \), then \( n \notin \mathbb{P} \). If \( n \equiv 1 \pmod{3} \), then \( n + 2 \equiv 0 \pmod{3} \) and so \( n + 2 \) is not a prime (since \( n + 2 > 3 \)). Lastly, if \( n \equiv 2 \pmod{3} \), then \( 5n + 2 \equiv 12 \equiv 0 \pmod{3} \), so \( 5n + 2 \) is not a prime (again, we are using that \( 5n + 2 > 3 \) too).

Exercise 1.8. We know that \( (a, b)[a, b] = ab \), and since \( [a, b] > \frac{ab}{2} \), this means that \( (a, b) < 2 \). Hence, this forces us to have \( (a, b) = 1 \).

### 2. Other practice problems

Exercise 2.1. False. This is because \((124, 1040) = 4\) which is not a divisor of 10.

Since there will less material on congruences, here is some more material on the previous chapter to help you.

Exercise 2.2. Let \( a \) and \( n \) be positive integers with \( a > 1 \). Prove that, if \( a^n + 1 \) is a prime, then \( a \) is even and \( n \) is a power of 2.

**Solution:** By contradiction, assume that \( a \) is odd or \( n \) is divisible by some odd positive integer. If \( a \) is odd, then \( a^n + 1 \) is even (but not 2 since \( a > 1 \)), and hence \( a^n + 1 \) is not a prime. If \( n \) is divisible by some odd positive integer, say \( c \), then we write \( n = bc \) for some positive integer \( b \). Next, from the homework, recall that we can factorize as

\[
a^{bc} + 1 = (a^b + 1)(a^{bc} - a^{b(c-1)} + \cdots - a + 1).
\]

This gives a factorization of \( a^n + 1 \) so that \( a^n + 1 \) is not a prime.

Exercise 2.3. Prove of disprove the following conjectures.

**Conjecture 2.1.** There are infinitely many prime numbers expressible in the form \( n^3 + 1 \) where \( n \) is a positive integer.

**Solution:** The first conjecture can be disproved by using the factorization \( n^3 + 1 = (n + 1)(n^2 - n + 1) \). This shows that the only prime number expressible in the desired form is 2 (with \( n = 1 \)). The second conjecture can be disproved by the counterexample \( n = 41 \).

Exercise 2.4 (Very important). (a) Let \( a, b, c \in \mathbb{Z} \) with \( (a, b) = 1 \) and \( a|bc \). Prove that \( a|c \). (b) Provide a counterexample to show why the statement of part (a) does not hold if \( (a, b) > 1 \).  

**Solution:** (a) Let \( m \) and \( n \) be integers for which \( ma + nb = 1 \) and let \( d \) be an integer for which \( bc = ad \). Then \( mac + nbc = c \) so that \( mac + nad = c \) or, equivalently, \( a(mc + nd) = c \) from which the desired result follows. (b) A counterexample is given by \( a = b = 2 \) and \( c = 1 \).

Exercise 2.5. Let \( n \in \mathbb{N} \). Then \( n \) is said to be **powerful** if all the exponents in the prime factorization of \( n \) are at least 2. Prove that a powerful number is the product of a perfect square and a perfect cube.

**Solution:** Let \( n \) be a powerful number and let \( n = p_1^{a_1}p_2^{a_2}\cdots p_r^{a_r} \) be its unique prime factorization. Without loss of generality, assume that the first \( s \) prime powers in the prime factorization of \( n \) have even exponents and that the last \( r - s \) prime powers have odd exponents. Then integers \( b_i \) exist such that

\[
n = p_1^{2b_1}p_2^{2b_2}\cdots p_s^{2b_s}p_{s+1}^{2b_{s+1} + 3}p_{s+2}^{2b_{s+2} + 3}\cdots p_r^{2b_r + 3} \\
= (p_1^{b_1}p_2^{b_2}\cdots p_r^{b_r})^2(p_{s+1}^{b_{s+1}}p_{s+2}^{b_{s+2}}\cdots p_r)^3,
\]

as desired. Note that here the integers \( b_{s+1}, b_{s+2}, \ldots, b_r \) must be assumed non-negative instead of strictly positive.