Recommended review exercises. Chapter 4

1(1), 7(4), 8(5), 14(6), 16(7)

Solutions:

1(1): Find the quotient and remainder when 11, 109, 999, 999, 997 is divided by 1111.

This is an application of the division algorithm, $a = qb + r$, $b = 1111$, $a = $

We can write

$$a = 11119999999997 - 10{,}000{,}000{,}000$$

and $10.000.000.000 = 9.999.999.999 + 1 = 9.999.999.900 + 100 =$

$$9{,}000{,}900 \cdot 1111 + 100$$

and

$$11119999999997 = 11119999999900 + 97 = 100090009 \cdot 1111 + 97$$

so that

$$a = (100090009 - 9000900) \cdot 1111 + 97 - 100$$

$$\begin{array}{r} 100090009 \\ -\ 9000900 \\ \hline 90909109 \end{array}$$

which yields

$$a = 90909109 \cdot 1111 - 3 = 90909108 \cdot 1111 + 1108$$

So $\underline{q = 90909108}$ and $\underline{r = 1108}$

7(4): Find $\gcd(2700, -504)$ and express it as a linear combination of the given integers.

We employ the Euclidean algorithm on 2700 and 504:

$$\begin{aligned} 2700 &= 5 \cdot 504 + 180 \\ 504 &= 2 \cdot 180 + 144 \\ 180 &= 1 \cdot 144 + 36 \\ 144 &= 4 \cdot 36 + 0 \end{aligned}$$

Last nonzero remainder = gcd

$$\begin{array}{r} 2700 \\ -\ 2520 \\ \hline 180 \end{array} \qquad \begin{array}{r} 504 \\ -\ 360 \\ \hline 144 \end{array}$$

So we have $\gcd(2700, 504) = \gcd(2700, -504) = \underline{36}$

Backtracking we get

$$36 = 180 - 1 \cdot 144 = 180 - 1 \cdot (504 - 2 \cdot 180) = 3 \cdot 180 - 1 \cdot 504 =$$

$$= 3 \cdot (2700 - 5 \cdot 504) - 1 \cdot 504 = 3 \cdot 2700 - 16 \cdot 504$$

so that

$$36 = 3 \cdot 2700 - 16 \cdot 504$$

giving

$$\underline{36 = 3 \cdot 2700 + 16 \cdot (-504)}$$

8(5): Suppose x, a, and b are integers such that $x | ab$. If x and a are relatively prime, prove that $x | b$.

[This is a classic property in the theory of divisors. It states that if there is nothing of x in a but x is in ab, then x must be totally in b.]

Proof: Since x and a are relatively prime we can find integers s&t such that $s \cdot a + t \cdot x = 1$. Multiplying with b we get $sab + txb = b$. Since $x | ab$ we can write $ab = q \cdot x$ giving

$$sqx + txb = b \iff b = x \cdot (sq + tb)$$

but this means that $x | b$ which completes the proof.

14(6): For any $k \in \mathbb{N}$, prove that $\gcd(4k+3, 7k+5) = 1$.

We can use the Euclidean algorithm (or almost*)

$$7k+5 = 1 \cdot (4k+3) + 3k+2$$

$$4k+3 = 1 \cdot (3k+2) + k+1$$

$$3k+2 = 3 \cdot (k+1) - 1$$

*This is really not the division algorithm since -1 is a negative number, however we can use this in the same way as when writing the gcd of other numbers as a linear combination of those numbers. That is we can write

$$-1 = (3k+2) - 3(k+1) = (3k+2) - 3 \cdot ((4k+3) - 1 \cdot (3k+2)) \Rightarrow$$

$$-1 = 4 \cdot (3k+2) - 3 \cdot (4k+3) = 4 \cdot ((7k+5) - 1 \cdot (4k+3)) - 3 \cdot (4k+3) \Rightarrow$$

$-1 = 4 \cdot (7k+5) - 7 \cdot (4k+3)$ which can also be written as

$$7 \cdot (4k+3) - 4 \cdot (7k+5) = 1,$$

this means that we have found m&n such that

$$m(4k+3) + n(7k+5) = 1$$

this means that every common divisor c of $4k+3$ and $7k+5$ must divide 1, that means that each common divisor of $4k+3$ and $7k+5$ must be 1 or -1, which means that the greatest common divisor of $4k+3$ and $7k+5$ is 1, which was what we wanted to prove.

(GCD = 1 is also termed "the numbers are relatively prime".)

16(7): (a) Give Euclid's proof that there are infinitely many primes.

We formulate it as a theorem:

Theorem: (Euclid) There are infinitely many prime numbers.

Proof: Assume the opposite, that is suppose that $p_1, p_2, \dots, p_N$ is a complete list of all prime numbers. Since $p_1, p_2, \dots, p_N$ is a complete list of all prime numbers, the integer

$$M = p_1 \cdot p_2 \cdot p_3 \cdot \dots \cdot p_N + 1$$

must not be a prime number since it is greater than all $p_1, p_2, \dots, p_N$. All integers except ± 1 are divisible by a prime number but M is not divisible by any prime number since M divided by any prime number always gives remainder 1. This is a contradiction. The assumption that there is a finite number of prime numbers must therefore be false which means that the number of prime numbers must be infinite. The proof is complete.

(b) State the Fundamental Theorem of Arithmetic

Theorem: Every integer $n \geq 2$ can be written

$$n = q_1^{\alpha_1} \cdot q_2^{\alpha_2} \cdot \dots \cdot q_s^{\alpha_s}$$

as the product of powers of distinct prime numbers $q_1, q_2, \dots, q_s$. The primes $q_1, q_2, \dots, q_s$ and the exponents $\alpha_1, \alpha_2, \dots, \alpha_s$ are unique.

Example:

$$360 = 36 \cdot 10 = 6 \cdot 6 \cdot 2 \cdot 5 = 2 \cdot 3 \cdot 2 \cdot 3 \cdot 2 \cdot 5 =$$

$$2^3 \cdot 3^2 \cdot 5^1 \longleftarrow \boxed{q_1 = 2,\ \alpha_1 = 3,\ q_2 = 3,\ \alpha_2 = 2,\ q_3 = 5,\ \alpha_3 = 1}$$

$$360 = 2 \cdot 180 = 2 \cdot 9 \cdot 2 \cdot 10 =$$

$$= 2 \cdot 3 \cdot 3 \cdot 2 \cdot 2 \cdot 5 = 2^3 \cdot 3^2 \cdot 5^1 \longleftarrow$$ The same factorization!