

1 Elementary number theory, V

The setup is the same as in Worksheets I, II, III and IV. You may assume all the Propositions from Worksheets I, II, III and IV. [But, be warned that you are expected to know the proofs of these, and we will be revisiting them.]

Definition 41. We say that integers a and b are **relatively prime** (or **co-prime**) if $\gcd(a, b) = 1$.

Corollary 42. Let a and b be integers, not both zero. Then $\gcd(a, b) = 1$ if and only if there exist integers x and y so that $ax + by = 1$.

Proposition 43. If n is an integer, then $\gcd(n, n + 1) = 1$.

Theorem 44. Let a, b and c be integers. If $a|bc$ and $\gcd(a, b) = 1$ then $a|c$.

Proposition 45. Let a and b be integers such that at least one of a and b is not zero. If $a = bq + r$ then $\gcd(a, b) = \gcd(b, r)$.

Example 46. Find $\gcd(835, 45)$, $\gcd(216, 57)$ and $\gcd(85, 31)$.

Exercise 47. Describe a method suggested by Proposition 45 for finding the greatest common divisor of two integers.

This method finds $\gcd(a, b)$ from a and b . Explain how it also finds x and y so that

$$ax + by = \gcd(a, b).$$

Theorem 48. Let a be an integer and n a natural number. If $\gcd(a, n) = 1$ then there exists an integer x such that $ax \equiv 1 \pmod{n}$.

Example 49. Let $a = 12$ and $n = 85$. Use what we now know to find an integer x so that $12x \equiv 1 \pmod{85}$.

Exercise 50. Find four examples of problems like Example 49. You should find a and n that are relatively prime, then find an integer x so that $ax \equiv 1 \pmod{n}$, for your choice(s) of a and n .

Make sure that your examples are not too easy, but also not too hard.

Question 51. Suppose that a and b are relatively prime integers. How many solutions (x, y) are there of the equation

$$ax + by = 1,$$

for x and y integers? Is the solution unique? Are there at most five solutions? Are there finitely many? Are there infinitely many?

Conjecture 52. Let a, b and c be integers with $c \neq 0$, and let n be a natural number. If $ac \equiv bc \pmod{n}$ then $a \equiv b \pmod{n}$.