1 Elementary number theory, IV

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

Definition 32. *Let a and b be integers and suppose that not both of a and b are zero. An integer d is a* **greatest common divisor** *of a and b if the following two statements are true:*

1. *$d|a$ and $d|b$;*
2. *for any integer c such that $c|a$ and $c|b$ we have $c \leq d$.*

Theorem 33. *Let a and b be integers such that not both are zero. Define a set*

$$D = \{am + bn \mid m, n \in \mathbb{Z}, am + bn > 0\}.$$

The following statements hold:

1. *D is a non-empty set of positive integers;*
2. *D has a smallest element $d > 0$;*
3. *There are integers x and y so that $d = ax + by$;*
4. *$d|a$;*
5. *$d|b$;*
6. *If c is any integer so that $c|a$ and $c|b$ then $c|d$;*
7. *If c is any integer so that $c|a$ and $c|b$ then $c \leq d$;*
8. *d is a greatest common divisor of a and b.*

Proposition 34. *Let a and b be integers which are not both zero. If d and d' are greatest common divisors of a and b, then $d = d'$.*

Remark 35. *Proposition 34 says that a greatest common divisor of a and b is unique.*

Notation 36. *The unique greatest common divisor of a and b is denoted* $\gcd(a, b)$.

Theorem 37. *Let a and b be integers, not both zero. Then* $\gcd(a, b)$ *is equal to the smallest element of the set*

$$D = \{am + bn > 0 \mid m, n \in Z\}.$$

Corollary 38. *Suppose that a and b are integers, not both zero. There are integers x and y so that*

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