1 Elementary number theory, VI

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

Definition 51. *We say that a natural number $n > 1$ is* **composite** *if n is the product of natural numbers less than n.*

Definition 52. *We say that a natural number $p > 1$ is* **prime** *if p is not the product of natural numbers less than p.*

Theorem 53. *Let $n > 1$ be a natural number. Then there exists a prime p such that $p|n$.*

Proposition 54. *Suppose that p is a prime and that a is a natural number. Then either $\gcd(a, p) = 1$ or $\gcd(a, p) = p$. The case $\gcd(a, p) = p$ happens if and only if $p|a$.*

Theorem 55. *Suppose that p is a prime, and that a and b are natural numbers. If $p|ab$ then $p|a$ or $p|b$.*

Remark 56. *Theorem 55 is called* Euclid's Lemma.

Theorem 57. *Suppose that p is a prime and let $\mathbf{Z}_p$ be the set of equivalence classes of integers modulo p. Then $\mathbf{Z}_p$ (with the usual operations of addition and multiplication) is a field.*

Theorem 58. *There are infinitely many prime numbers.*