Cheatsheet on arithmetic

Erwann Rogard

2020/10/11

Abstract

Hints rather than complete proofs. Since these are common, by default no source.

Contents

1 Bézout and derivatives **2**

1 Bézout and derivatives

Result 1 (Bézout identity)**.** *Let* $a, b \in \mathbb{N}^+$*, and* $c = \gcd(a, b)$*, then there exists* $u, v \in \mathbb{Z}^*$ *such that* $c = a \times u + b \times v$*.*

Proof. Trivially, *i)* $L^+ \neq \emptyset$, thus admits a minimum by the well ordering principle. *ii)* c divides a and b, thus divides d, and $c \leq d$. But also, *iii)* d divides a, as assuming otherwise leads to a contradiction. And, by symmetry, *iv)* d divides b. Altogether, *v)* d divides c, and $d \leq c$. In all, $d = c$. □

Result 2 (Mutually primes)**.** $a, b \in \mathbb{N}^+$ *are mutually primes if and only if there exists* $u, v \in \mathbb{Z}$ $a \times u + b \times v = 1$

Proof. Follows from 1 □

Result 3 (Gauss' lemma)**.** $a, b, c \in \mathbb{N}^+$ *and* a *divides* $b \times c$*, and* a *and* b *are mutually primes, then* a *divides* c*.*

Proof. Follows from 1 and 3 □