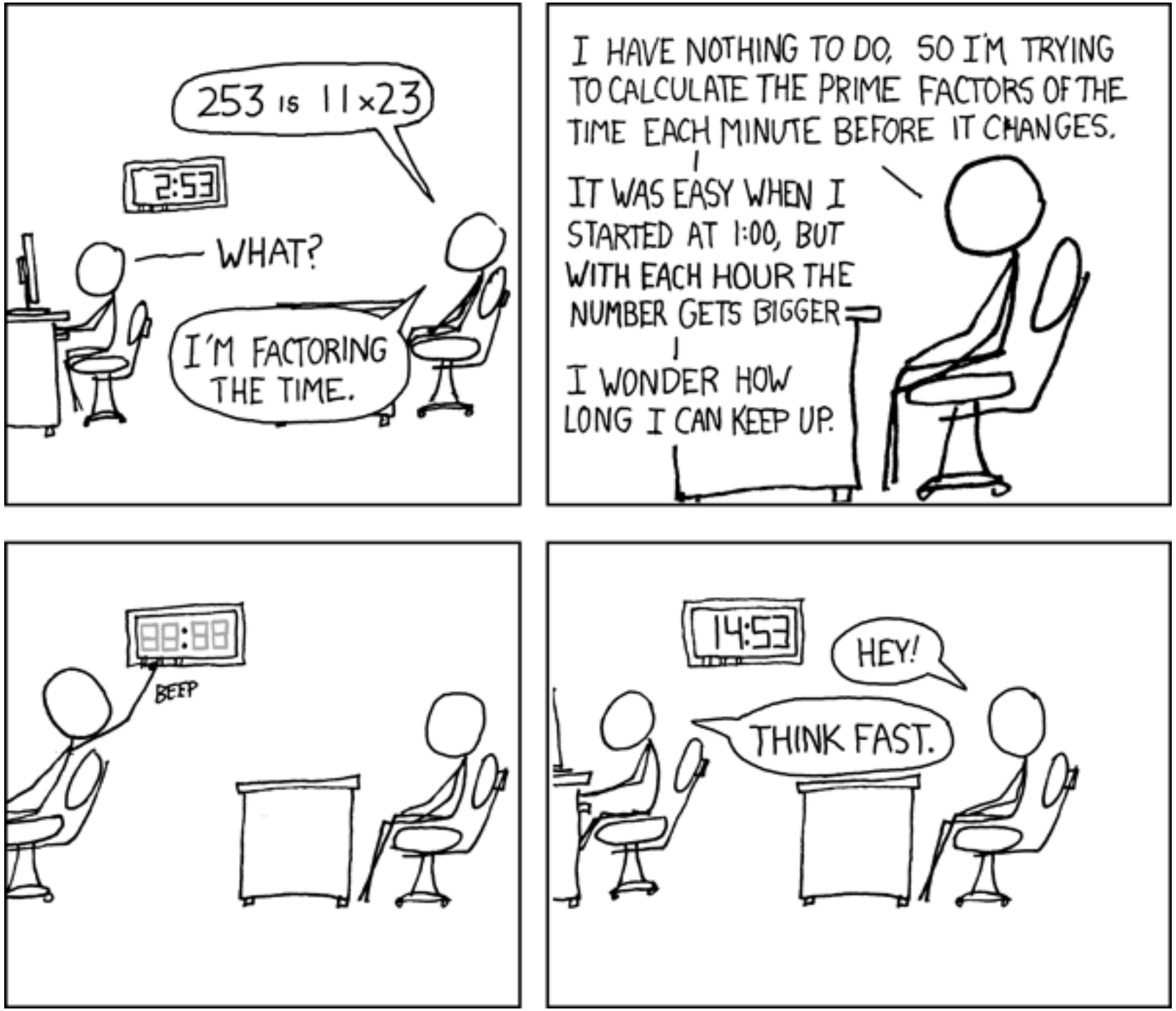
Divisibility in Rings

Petr Samodelkin
Elias Köhnlein



The Definitions

Definition 1. Divides:

Mathematical Expression

We define $x \mid y$ if $\exists a, y = a \cdot x$

Lean Code

```
def Divides (x y : R) :
Prop :=
∃ a, y = a * x

notation x " | " y =>
 Divides x y
```

Definition 2. Unit:

Mathematical Expression

We say *a* is a unit, if it has an multiplicative inverse:

$$\exists\, b \in R : a \cdot b = b \cdot a = 1$$

Example:

In Z_{10}: 2, 4 and 5 *aren't* units, but 1, 3, 7, 9 are.

Lean Code

In-Built:

a is a unit, if there's an element of R^x which equals a.

Elements of R^x have double-sided inverses by definition.

Definition 2. IsAssociated:

Mathematical Expression

x and y are associated if there exists a unit a, such that:

$$y = a \cdot x$$

In Z_{10}, 2, 4, 6, 8 are associated:

$2 * 3 \equiv 6$, $6 * 7 \equiv 2$.

$2 * 7 \equiv 4$, $4 * 3 \equiv 2$

Lean Code

```
def IsAssociated (x y : R):
Prop :=
∃ (a : R), y = a * x

lemma
isAssociated_is_symmetric

lemma
isAssociated_is_transitive
```

Definition 3. IsNontrivial:

Mathematical Expression

x is nontrivial if x ≠ 0 and
¬(IsUnit x)

Lean Code

```
def IsNontrivial (x : R)
 Prop := x ≠ 0 ∧
            ¬(IsUnit x)
```

Definition 4. IsIrreducible:

Mathematical Expression

x is irreducible, if:

1. x is nontrivial
2. For any a, b in R, such that a*b=x, one of them is a unit.

=>it cannot be factored in 2 non-unit elements.

Lean Code

```
def IsIrreducible (x : R) :
 Prop :=
 IsNontrivial x ∧ ∀ a b,
 x = a ∗ b →
 IsUnit a ∨ IsUnit b
```

Definition 5. IsPrime:

Mathematical Expression

x is prime if

1. x is nontrivial, and
2. Euclid’s lemma applies:

   If x divides *ab,* it divides either *a* or *b.*

Lean Code

```
def IsPrime (x : R) :
 Prop :=
IsNontrivial x ∧ ∀ a b,
 (x ∣ a * b) → (x ∣ a)
 ∨ (x ∣ b)
```

The two Theorems

Theorem 1. Every Prime Element is Irreducible in an Integral Domain

Formal Statement:

Let R be an integral domain and $x \in R$.

If x is prime, then x is irreducible.

Theorem 1: LaTeX proof

1. In an integral domain, every prime element is irreducible.

   Proof:

   Let R be an integral domain and $x \in R$ a prime element. We show that x is irreducible:

   1. Let $x = a \cdot b$ for $a, b \in R$.
   2. Since x is prime, from $x \mid a \cdot b$, it follows that $x \mid a$ or $x \mid b$.
   3. Assume $x \mid a$. Then there exists $c \in R$ with $a = c \cdot x$.
   4. Set $x = a \cdot b = (c \cdot x) \cdot b = x \cdot (c \cdot b)$.
   5. Since R is an integral domain and $x \neq 0$, it follows $c \cdot b = 1$. Thus, b is a unit.
   6. Similarly, a is a unit if $x \mid b$.
   7. Therefore, x is irreducible.

Theorem 1: Lean 4 code

```
theorem isIrreducible_of_isPrime [IsDomain R] (x : R) (h : IsPrime x) : IsIrreducible x := by
  obtain ⟨hnontrivial, hdiv⟩ := h — x nontrivial and x|a*b
  constructor
  · exact hnontrivial
  · intros a b h_mul
    -- x divides a * b, as x = a * b
    have hx_divides_ab : x | a*b := by
        use 1; simp[h_mul]
    have hxa_or_xb := hdiv a b hx_divides_ab -- x divides either a or b because it's prime
    rcases hxa_or_xb with hxa | hxb -- if x | a, substitute a = c * x, to get x = x * (c * b)
    · exact Or.inr (is_unit_of_mul_eq_one h_mul hnontrivial hxa)
    · have h_mul1 : x = b * a := by -- same here
          simp[mul_comm, h_mul]
      exact Or.inl (is_unit_of_mul_eq_one h_mul1 hnontrivial hxb)
```

Theorem 1: Lean 4 code

```
lemma  is_unit_of_mul_eq_one [IsDomain R] {a b x: R} (h_mul : x = a * b)
(hnontrivial: IsNontrivial x) (hxa: Divides x a) : IsUnit b := by
  -- we have x|a, x=ab, x ≠ 0
  obtain ⟨c, hxa⟩ := hxa -- a = c * x
  rw [hxa, mul_comm, ←mul_assoc] at h_mul -- rewrite to a * b = x = b * c * x
  have hbc1 : b * c = 1 := by -- x * y = x and x ≠ 0 => y = 1
        apply (mul_eq_right₀ hnontrivial.left).mp
        rw[←h_mul]
  exact isUnit_of_mul_eq_one b c hbc1 -- in-built lemma: b * c = 1 → b is unit
```

Definition 6. Unique factorization domain

Mathematical expression

A ring D is UFD if:

- It’s an integral domain
- Every non-zero, non-unit element is factorable into irreducibles
- such factorization is unique up to associates and permutation

Lean code:

Wait for it...

Definition 6. IsFactorialRing: Lean

```
def IsUFD (D: Type) [CommRing D] [IsDomain D]: Prop :=
  -- It's based on an integral domain D
  -- every non-trivial element is factorable into irreducibles
  (∀ (x : D), x ≠ 0 → ¬IsUnit x → ∃ (factors :List D), -- for any non-zero, non-unit x in D there's a list
  ((∀ y ∈ factors, IsIrreducible y) ∧ x=List.prod factors)) ∧ -- of irreducibles that multiply to x
  -- And such factorisation is unique up to associates and permutation:
  (
  ∀ (x : D) (factors1 factors2 : List D), -- for any x in D, if there exist 2 lists
  x ≠ 0 → (¬IsUnit x) → -- such that x is non-zero and non-unit
  (x = List.prod factors1) → (x = List.prod factors2) → -- that x is the product of the factors in each list
  (∀ y ∈ factors1, IsIrreducible y) → (∀ y ∈ factors2, IsIrreducible y) → -- and those lists are made up of irreducibles
  ((factors1.length=factors2.length) ∧ -- then they are of equal length
  ∃ σ ∈ factors1.permutations, -- and there exists a permutation of one of them, here called sigma
  (∀ i : Fin σ.length,  (IsAssociated (σ.get i) (factors2.get! i )))) -- such that sigma[i] is associated to factors2[i]
  )
```

Theorem 2 : Statement

- In a unique factorization domain, every irreducible element is prime.
- Counterexample in non-UFD:

> let $R = \mathbb{Q} + x\mathbb{R}[x]$, i.e. the ring of real polynomials with rational constant coefficient. Then x is irreducible but not prime, since $x \mid (\sqrt{2}x)^2$ but $x \nmid \sqrt{2}x$, by $\sqrt{2} \notin \mathbb{Q}$.

Theorem 2: LaTeX Proof

Proof:

1. Let p irreducible, and $pc = ab$. We need to show that $p|a \vee p|b$.
2. a and b are non-zero and non-unit:
    1. Case 1: $a = 0$, then $p|a$, similarly for b.
    2. Case 2: a is a unit, then we can rearrange $pc = ab$ to $b = pa^{-1}c \implies p|b$.
3. c is also non-zero and non-unit:
    1. a and b are non-zero, therefore $ab = pc \neq 0$ and thus $c \neq 0$.
    2. If c is a unit, then pc is irreducible, and either a or b is a unit, so c is not a unit.
4. Since D is a UFD, there exist unique factorisations: $a = a_1a_2 \dots a_r$, $b = b_1b_2 \dots b_s$, $c = c_1c_2 \dots c_t$.
   Since ab is non-trivial, and

   $$ab = c_1c_2 \dots c_t \cdot p = a_1a_2 \dots a_r \cdot b_1b_2 \dots b_s$$

   p must be an associate of one of a_i or b_i.
5. Suppose $up = a_i$, where u is a unit. Then rewriting a as $a = a_1a_2 \dots a_{i-1}pu \cdot a_{i+1} \dots a_r$ shows $p|a$. Similarly, if $up = b_i$, $p|b$. Thus, p is prime.

Thank you for your attention!