Sølvkorn 14
The final word on prime lemmas (for now)

Rasmus Sylvester Bryder

An integer $n \in \mathbb{Z}$ is *square-free* if it holds for any $m \notin \{-1, 1\}$ that $m^2 \nmid n$.

Recall that for any integers x and y with greatest common divisor d, **Bézout's identity** yields existence of integers a and b such that $ax + by = d$. In particular, x and y are relatively prime (i.e. their greatest common divisor is 1) if and only if there exist integers a and b such that $ax + by = 1$. Recall also that for any integer x with $|x| > 2$ there exists a prime number dividing x.

A prime number p and any integer x are relatively prime if and only if $p \nmid x$. This is easy to prove: if $p \mid x$, then p and x are clearly not relatively prime, and if p and x are not relatively prime, there exists a prime number q such that $q \mid p$ and $q \mid x$. Hence $q = p$, so $p \mid x$.

This famous lemma follows from the above observation:

Euclid's lemma. *Let n, x and y be integers. If $n \mid xy$ and n and x are relatively prime, then $n \mid y$. (In particular, if p is prime and $p \mid xy$, then $p \mid x$ or $p \mid y$.)*

Proof. Take $a, b \in \mathbb{Z}$ such that $ax + bn = 1$ by means of Bézout's identity. Then $axy + bny = y$. Since $n \mid xy$ and $n \mid bny$, it follows that $n \mid y$. □

We will first ask ourselves how square-free integers look.

Lemma 1. *Let $n \in \mathbb{Z}$. Then the following are equivalent:*

(i) *n is a square-free integer.*
(ii) *$n = 1$, $n = -1$ or $n = sp_1 \cdots p_m$ for different prime numbers $p_1, \ldots, p_m$ and some $s \in \{-1, 1\}$.*

Proof. Assume that (i) holds and that $x \notin \{-1, 1\}$. As $x \neq 0$, we must have $|x| > 2$, so there exist $s \in \{-1, 1\}$, different prime numbers $p_1, \ldots, p_m$ and positive integers $\alpha_1, \ldots, \alpha_m$ such that

$$n = sp_1^{\alpha_1} \cdots p_m^{\alpha_m}.$$

As n is square-free, we cannot have $\alpha_i \geq 2$ for any i, so $\alpha_1 = \cdots = \alpha_m = 1$. Hence (ii) follows. If (ii) holds, note that 1 and -1 are clearly square-free integers. In the case $n = sp_1 \cdots p_m$ as in (ii), note that if $m \in \mathbb{Z} \setminus \{-1, 1\}$ satisfies $m^2 \mid n$, then there is a prime number $p \in \mathbb{N}$ such that $p \mid m$ and therefore $p^2 \mid n$. Hence there exists $q \in \mathbb{Z}$ such that $p^2 q = n$. As $p \mid n$, Euclid's lemma yields that $p \mid p_i$ for some $i = 1, \ldots, m$. Hence $p = p_i$, so

$$p_i^2 q = sp_1 \cdots p_m.$$

Dividing by p_i, p_i must now divide one of the factors on the right hand side which is clearly impossible as all the prime numbers are different from p_i by assumption. Hence $m^2 \nmid n$, so n is square-free. □

The importance of square-free integers will be more pronounced in this next theorem.

Theorem 2. *Let $n \in \mathbb{Z}$ be non-zero. Then there exist a $y \in \mathbb{N}$ and a square-free integer $x \in \mathbb{Z}$ such that n can be decomposed as $n = xy^2$. Moreover, x and y are uniquely determined.*

Proof. Existence. If $|n| = 1$ we put $x = n$ and $y = 1$. Hence we can assume that $|n| > 1$. Therefore there exist $s \in \{-1, 1\}$, different prime numbers $p_1, \ldots, p_m$ and positive integers $\alpha_1, \ldots, \alpha_m$ such that

$$n = sp_1^{\alpha_1} \cdots p_m^{\alpha_m}.$$

For all $i \in 1, \ldots, m$, let β_m be the largest non-negative integer such that $2\beta_i \leq \alpha_i$ and let $\gamma_i = \alpha_i - 2\beta_i$. Note now that if we define $x = sp_1^{\gamma_1} \cdots p_m^{\gamma_m}$ and $y = p_1^{\beta_1} \cdots p_m^{\beta_m}$ then

$$n = (p_1^{\gamma_1} \cdots p_m^{\gamma_m})(p_1^{\beta_1} \cdots p_m^{\beta_m})^2 = xy^2.$$

By definition of the γ_i, we see that $\gamma_i \in \{0, 1\}$ for all i. Hence

$$x = s \prod_{\substack{1 \leq i \leq m \\ \gamma_i \neq 0}} p_i,$$

so by Lemma 1, x is square-free. Hence existence follows.

Uniqueness. Assume that $n = xy^2$ and $n = x_1 y_1^2$ where x and x_1 are square-free integers and y and y_1 are positive integers. Let d be the greatest common divisor of y and y_1 and let $n_1 = \frac{n}{d^2}$, $z = \frac{y}{d}$ and $z_1 = \frac{y_1}{d}$. Bézout's identity immediately yields $a, b \in \mathbb{Z}$ such that $az + bz_1 = 1$. Cubing both sides yields

$$z^2(a^3 z + 3ba^2 z_1) + z_1^2(3ab^2 z + b^3 z_1) = (az)^3 + 3(az)^2 bz_1 + 3az(bz_1)^2 + (bz_1)^3 = 1,$$

so that z^2 and z_1^2 are relatively prime. Since $xz^2 = n_1 = x_1 z_1^2$, then $z^2 \mid x_1$ by Euclid's lemma. Since x_1 is square-free we cannot have $|z| > 1$, so $|z| = 1$ and hence $z = 1$ since z is positive. Similarly $z_1^2 \mid x$, implying $z_1 = 1$. Therefore $x = n_1 = x_1$ and $y = dz = dz_1 = y_1$. □

The final statement of this nugget will be a generalization of a very well-known statement, namely that $\sqrt{2}$ is irrational.

Lemma 3. *Let $n \in \mathbb{N}$. Then the following are equivalent:*

(i) *$\sqrt{n}$ is rational.*
(ii) *$n = m^2$ for some $m \in \mathbb{N}$.*

Hence for any $n \in \mathbb{N}$, $\sqrt{n}$ is either irrational or an integer.

Proof. It is clear that (ii) implies (i). Assume that (ii) does not hold and write $n = xy^2$ for a positive square-free integer x and some $y \in \mathbb{N}$ by means of the above theorem. It is clear that $x \neq 0$ and since (ii) does not hold, we have $x \neq 1$ as well. Therefore $x \geq 2$, so $x = p_1 \cdots p_n$ for different prime numbers $p_1, \ldots, p_n$ by Lemma 1. Let $p = p_1$.

Assume now that $\sqrt{x} = \sqrt{n}/y$ is rational and write $\sqrt{x} = r/s$ for relatively prime numbers $r, s \in \mathbb{N}$. Then $r^2 = xs^2$. As p divides the right hand side, p divides r^2 as well. Hence $p \mid r$ by Euclid's lemma, so we can write $r = r_1 p$ for some $r_1 \in \mathbb{N}$. Therefore $m^2 p^2 = xq^2$ or $r_1^2 p = p_2 \cdots p_m s^2$ after dividing by p. Thus p divides the right hand side; Euclid's lemma yields that $p \mid s^2$, since p cannot divide $p_2, \ldots, p_m$. Euclid's lemma now yields $p \mid s$, but this contradicts the fact that r and s are relatively prime. Hence $\sqrt{x}$ is irrational, so $\sqrt{n} = y\sqrt{x}$ is irrational as well, proving that (i) does not hold. □