RATIONAL ROOTS
DONU ARAPURA

Let \( f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0 \) be a polynomial with integer coefficients. A number \( r \) such that \( f(r) = 0 \) is called a root. We'll mainly be interested in rational roots. In this case we have:

**Proposition 1.** (The rational root test) Any rational solution of \( f(x) = 0 \) is automatically an integer.

**Proof.** Let \( r = \frac{b}{c} \) be root where \( b \) and \( c \) are integers with \( c > 0 \) and \( \gcd(b, c) = 1 \).

Suppose that \( r \) is not an integer, then \( c \neq 2 \). Multiplying \( f(r) \) by \( c^n \) yields:

\[
b^n + a_{n-1}b^{n-1}c + \ldots + a_0c^n = 0.
\]

After isolating \( b^n \) on one side of the equation, we see that \( c \) divides it. This implies that any prime factor say \( p \) of \( c \) divides \( b^n \). Since \( p \) is prime, it must actually divide \( b \). Therefore \( p \) is common factor of \( b \) and \( c \) contrary to our assumptions. So \( r \) must be an integer.

We consider some methods to determine what the integers roots are, or if such roots exist?

**Trial and Error with bounds**

The idea is simply to substitute various integers \( 0, \pm 1, \ldots \) into \( f(x) \) until we find a root. If we find a root say \( r \), then divide \( f(x) \) by \( (x - r) \) and repeat. We need to be able to decide when to stop. Here's a simple test:

**Proposition 2.** Let \( R \) be the maximum of \( \frac{|a_{n-1}|}{n}, \frac{|a_{n-2}|}{n^{1/2}}, \frac{|a_{n-3}|}{n^{1/3}}, \ldots \). The any real (e.g. integer) root \( r \) must satisfy \( -R \leq r \leq R \).

**Proof.** Suppose \( |r| > R \), then

\[
\frac{|a_{n-1}|}{r} < \frac{|a_{n-1}|}{R} \leq \frac{1}{n}
\]

because \( R > |a_{n-1}|n \). Similarly,

\[
\frac{|a_{n-2}|}{r^2} < \frac{|a_{n-1}|}{R^2} \leq \frac{1}{n}
\]

and so on. Therefore

\[
\frac{|a_{n-1}|}{r} + \frac{|a_{n-2}|}{r^2} + \ldots \leq \frac{|a_{n-1}|}{r} + \frac{|a_{n-2}|}{r^2} + \ldots < \frac{1}{n} + \frac{1}{n} + \ldots = 1.
\]

Consequently

\[
\frac{f(r)}{r^n} = 1 + \frac{a_{n-1}}{r} + \frac{a_{n-2}}{r^2} + \ldots > 0.
\]

So \( r \) cannot be a root. \( \square \)
Example 1. Let \( f(x) = x^3 + 4x + 15 \). Then \( R \) is the max. of 0, \( \sqrt{12} \) and (45)\(^{1/3} \) which is less than 4. Checking that \( f(x) \neq 0 \) for \( x = 0, \pm 1, \pm 2, \pm 3 \) (the work can be cut in half by observing that \( f(x) > 0 \) when \( x > 0 \)) shows that \( f \) has no rational roots.

Congruences

Let \( n \) be an integer greater than 1. Given integers \( x \) and \( y \), we say that \( x \) is congruent to \( y \) modulo \( n \) or

\[
x \equiv y \pmod{n}
\]

when \( x - y \) is divisible by \( n \).

Theorem 1. The following properties hold.

1. \( x \equiv x \pmod{n} \).
2. If \( x \equiv y \pmod{n} \) then \( y \equiv x \pmod{n} \).
3. If \( x \equiv y \pmod{n} \) and \( y \equiv z \pmod{n} \) then \( x \equiv z \pmod{n} \).
4. If \( x \equiv y \pmod{n} \) and \( x' \equiv y' \pmod{n} \), then \( x + x' \equiv y + y' \pmod{n} \) and \( xx' \equiv yy' \pmod{n} \).

Proof. We’ll prove only a couple of lines. The rest are left as an exercise.

3. If \( x \equiv y \pmod{n} \) and \( y \equiv z \pmod{n} \) then \( n \) divides \( (x - y) \) and \( (y - z) \). Therefore \( n \) divides \( (x - z) = (x - y) + (y - z) \), so \( x \equiv z \pmod{n} \).

5. If \( x \equiv y \pmod{n} \) and \( x' \equiv y' \pmod{n} \), then \( (x - y) = na \) and \( (x' - y') = na' \). So \( xx' - yy' = (na + y)(na' + y') - yy' = n(naa' + ay' + a'y) \) is divisible by \( n \).

Given an integer \( x \), let \( \bar{x} \) denote the remainder of \( x \) after dividing by \( n \) (as described in the division algorithm). This is the unique integer between 0 and \( n - 1 \) such that \( x \equiv \bar{x} \pmod{n} \). Let

\[
\mathbb{Z}/n\mathbb{Z} = \{0, 1, \ldots, n - 1\}
\]

The rule for addition and multiplication are

\[
x + y = \bar{x} + \bar{y}
\]

and

\[
xy = \bar{x}\bar{y}
\]

(don’t confuse these with ordinary arithmetic). For example, \( 3 \cdot 5 = 1 \) in \( \mathbb{Z}/7\mathbb{Z} \).

With these operations \( \mathbb{Z}/n\mathbb{Z} \) becomes a commutative ring. Given a polynomial \( f(x) = x^n + a_n x^{n-1} + \ldots + a_0 \), let \( \bar{f}(x) = x^n + \bar{a}_n x^{n-1} + \ldots + \bar{a}_0 \). This is a polynomial with coefficients \( \mathbb{Z}/n\mathbb{Z} \) (in particular, we evaluate this using the rules of arithmetic in this ring). Now comes the main point.

Lemma 1. Let \( r \) be an integer root of \( f(x) \), then \( \bar{r} \) is root of \( \bar{f}(x) \) in \( \mathbb{Z}/n\mathbb{Z} \).

Proof. We have \( \bar{r}^2 = \bar{r}\bar{r} = \bar{r}^2 \) and \( \bar{r}^3 = \bar{r}\bar{r}\bar{r} = \bar{r}^3 \) and so on. Therefore

\[
\bar{f}(r) = r^n + a_n r^{n-1} + \ldots + a_0 = r^n + \bar{a}_n \bar{r}^{n-1} + \ldots + \bar{a}_0 = \bar{f}(\bar{r})
\]

Therefore \( \bar{f}(\bar{r}) = 0 = 0 \) if \( r \) is a root.

Example 2. Let \( f(x) = x^4 + 3210x^3 + 3001 \). Choose \( n = 3 \). Then \( \bar{f} = x^4 + 1 \). In \( \mathbb{Z}/3\mathbb{Z} \), one gets \( \bar{f}(0) = 1 \), \( \bar{f}(1) = 2 \), \( \bar{f}(2) = 2 \) so \( f \) has no integer roots.
Exercises
1. Finish the proof of theorem 1.
2. Determine the rational roots of \(x^5 - 1\).
3. Show that \(f(x) = x^3 + 420x^2 + 423\) has no rational roots by working in \(\mathbb{Z}/7\mathbb{Z}\).