# Polynomial Division in Number Theory

James Rickards

Canadian Winter Camp 2017

## 1 Introduction

One technique which can be very useful in solving number theory problems is the use of polynomial division. With some careful algebra and a will to carry on, you can solve some difficult problems without any tricky ideas. The general setup is when you know that a quotient of two expressions is an integer. The method you use is to find an approximation to what the quotient should be, ideally involving "nice" terms and a "nasty" term, where the nasty term is small. We then impose the conditions of the quotient being in $\mathbb{Z}$ to deduce what the nasty term should be, and then we have nice algebraic equations to work with.

A classical example looks like the following: Find all integers $x$ such that

$$\frac{3x^3 - 5x + 1}{2x - 1} = Q \in \mathbb{Z}.$$

For this problem, it's best to multiply by 8 to get

$$8Q = \frac{24x^3 - 40x + 8}{2x - 1} = 12x^2 + \frac{12x^2 - 40x + 8}{2x - 1} = 12x^2 + 6x + \frac{-34x + 8}{2x - 1} = 12x^2 + 6x - 17 + \frac{-9}{2x - 1}$$

Since $Q, x$ are integers, we see that $\frac{-9}{2x-1}$ is an integer, which reduces us to finitely many cases: $2x - 1 = -9, -3, -1, 1, 3, 9$, so $x = -4, -1, 0, 1, 2, 5$. In each of these cases we have shown that $8Q \in \mathbb{Z}$, but since the denominator of $Q$ in lowest terms is a divisor of $2x - 1$ which is odd, this implies that $Q \in \mathbb{Z}$. Thus $x = -4, -1, 0, 1, 2, 5$ is the set of solutions.

## 2 An Example

Let's go on to a more difficult example: the famous IMO 1988 problem 6: Let $a, b$ be two positive integers such that $ab + 1 \mid a^2 + b^2$. Prove that

$$\frac{a^2 + b^2}{ab + 1}$$

is a perfect square. The normal technique used to solve this problem is *Vieta jumping*. While this is a very standard trick now, back in the day it wasn't well known, and as such this problem was very difficult. The solution we give here will be somewhat similar, but not requiring any clever ideas.

To start off, suppose WLOG that $b \geq a$. Thus the $b$ term is the "dominant term", and to get a small term in the numerator we wish to eliminate that.

$$Q = \frac{a^2 + b^2}{ab + 1} = \frac{b}{a} + \frac{-\frac{b}{a} + a^2}{ab + 1} = \frac{b}{a} + \frac{a^3 - b}{a^2b + a}.$$

Since $a \leq b$, we see that either $0 \leq a^3 - b < a^3 \leq a^2b < a^2b + a$ or $0 \leq b - a^3 < b < a^2b + a$. In any case, we have a "nice" term of $\frac{b}{a}$ and a "nasty" term $\frac{a^3-b}{a^2b+a}$ which satisfies

$$\left| \frac{a^3 - b}{a^2b + a} \right| < 1.$$

In particular, $Q \sim \frac{b}{a}$; it is the ceiling or floor of $\frac{b}{a}$ if $a^3 - b \geq 0$ or $a^3 - b \leq 0$ respectively. Thus it is natural to write $b = an + r$, where $n \in \mathbb{Z}^+$ and $r \in \mathbb{Z}$, $0 \leq r < a$. We must get $Q = n$ or $Q = n + 1$, and plugging in the expression for $b$ yields

$$Q = n + \frac{r}{a} + \frac{a^3 - an - r}{a(na^2 + ra + 1)} = n + \frac{(nra^2 + r^2a + r) + (a^3 - an - r)}{a(na^2 + ra + 1)} = n + \frac{a^2 + nra + r^2 - n}{na^2 + ra + 1}.$$

Therefore $\frac{a^2+nra+r^2-n}{na^2+ra+1} = 0, 1$.

If it is 0, then note our expression is linear in $n$ and we solve to get

$$n = \frac{a^2 + r^2}{1 - ar}.$$

But $n > 0$ whence $1 \geq 1 - ar > 0$, so $ar = 0$ and thus $r = 0$. This gives $n = a^2$ and $Q = n = a^2$ is a perfect square (this is the solution $(a, b) = (a, a^3)$).

The other case is $\frac{a^2+nra+r^2-n}{na^2+ra+1} = 1$. When we multiply out, it is again linear in $n$, and we solve to get

$$Q = n + 1 = 1 + \frac{a^2 + r^2 - ra - 1}{a^2 - ra + 1} = \frac{2a^2 + r^2 - 2ar}{a^2 - ra + 1} = \frac{(a - r)^2 + a^2}{(a - r)a + 1}$$

where $a, a - r \in \mathbb{Z}^+$. In particular, starting with the pair $(a, b) = (a, an + r)$ we get $(a - r, a)$ giving the same quotient. However this decreases the sum $a + b$ (except if $a = b$, where we can check $(1, 1)$ is they only such possibility; this gives a quotient of 1), whence we can only do this finitely many times, whereupon we must be in the first case or $a = b = 1$, and the quotient is a square in both cases. Note that our solution also describes how to find all possible pairs $(a, b)$ where $ab + 1 \mid a^2 + b^2$.

# 3 Problems

1. a) Find infinitely many pairs of integers $a, b$ with $1 < a < b$ such that $ab \mid a^2 + b^2 - 1$
b) For $a, b$ as in part a), find the possible values of

$$\frac{a^2 + b^2 - 1}{ab}$$

which occur for infinitely many pairs $(a, b)$.

2. Find all pairs of positive integers $(a, b)$ such that

$$\frac{a^2 + b}{b^2 - a}, \frac{b^2 + a}{a^2 - b} \in \mathbb{Z}$$

3. Consecutive positive integers $m, m + 1, m + 2, m + 3$ are divisible by consecutive odd positive integers $n, n + 2, n + 4, n + 6$ respectively. Find the smallest possible $m$ in terms of $n$.

4. Let $x, y$ be integers such that $xy + 1 \mid x^2 + y^2$. Prove that if

$$N := \frac{x^2 + y^2}{xy + 1} < 0,$$

then $N = -5$.

5. Find all $a \in \mathbb{Z}$ such that

$$x^2 + axy + y^2 = 1$$

has infinitely many distinct integer solutions $(x, y)$.

6. Find all pairs of positive integers $(a, b)$ such that

$$a^2b + b + 7 \mid ab^2 + a + b$$

7. Find all positive integers which can be represented uniquely as

$$\frac{x^2 + y}{xy + 1},$$

for $x, y$ positive integers.

8. Let $x, y$ be positive integers such that $xy \mid x^2 + y^2 + 1$. Prove that

$$\frac{x^2 + y^2 + 1}{xy} = 3$$

9. Find all pairs of positive integers $(a, b)$ such that

$$ab \mid a^2 + b^2 + 3.$$

NOTE: you can leave your answer in terms of a set of recursive sequences.

10. Find all pairs of positive integers $(m, n)$ such that

$$\frac{n^3 + 1}{mn - 1} \in \mathbb{Z}.$$

11. Find all pairs of integers $(a, b)$ such that

$$\frac{a^2}{2ab^2 - b^3 + 1} \in \mathbb{Z}^+.$$

12. Determine all triples $(a, b, c)$ of positive integers such that each of the numbers

$$ab - c, bc - a, ca - b$$

is a power of 2.

12'. Prove that there are no quadruples $(p, a, b, c)$ where $p$ is an odd prime and $a, b, c \in \mathbb{Z}^+$ such that each of the numbers

$$ab - c, bc - a, ca - b$$

is a power of $p$.

12". Let $a \leq b \leq c$ be positive integers and $p$ a prime such that each of the numbers

$$-(ab - c), bc - a, ca - b$$

is a power of $p$. Prove that either $(a, b, c) = (p^u, p^u, p^{2u} + 1)$ for some non-negative integer $u$, or $a = 1$.