Polynomial Division in Number Theory

James Rickards

1 Introduction

Polynomial division is a useful technique in mathematics, which can be used to solve many algebra problems. Lesser known however is its power to solve difficult number theoretic problems, where the normally tricky ideas now naturally appear as a result of the algebra. The general setup is when you are given an expression involving a quotient of two polynomials, and the assertion that the quotient is an integer. The question will typically be along the lines of “find all solutions to this assertion”, or “prove some property of the quotient”. The method of solution is to polynomially divide and find an approximation to what the quotient should be, ideally involving “good” terms and a “bad/ugly” term, where the bad term is small. We then impose the conditions of the quotient being an integer to deduce what the bad term should be, from which we get nice algebraic equations to work with. Let’s call this method the “division method” for this article.

A classical example looks like the following:

**Problem 1:** Find all integers $x$ such that

$$Q := \frac{3x^3 - 5x + 1}{2x - 1}$$

is an integer.

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

$$8Q = \frac{24x^3 - 40x + 8}{2x - 1}$$

$$= 12x^2 + \frac{12x^2 - 40x + 8}{2x - 1}$$

$$= 12x^2 + 6x + \frac{-34x + 8}{2x - 1}$$

$$= 12x^2 + 6x - 17 + \frac{-9}{2x - 1}.$$ 

Here, $12x^2 + 6x - 17$ is the good term and $\frac{-9}{2x - 1}$ is the bad term. 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 the odd number $2x - 1$, this implies that $Q \in \mathbb{Z}$. Thus $x = -4, -1, 0, 1, 2, 5$ is the set of solutions.
2 A Typical Example

Let’s go on to a more difficult example: the famous IMO 1988 problem 6.

**Problem 2:** 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, in 1988 it wasn’t well known, and this was a very difficult problem. It even stumped future Fields Medalist Terence Tao! The basic idea behind Vieta jumping is you start with the “smallest” solution disproving the given assertion, and manipulate the assertion into a quadratic equation in some variable. Using Vieta’s formulas, you construct a smaller solution, giving a contradiction. The reader seeking a longer exposition on Vieta jumping can start with the article by Yimin Ge, found on his website (http://www.yimin-ge.com/doc/VietaJumping.pdf). The solution we give here will be somewhat similar, but where the clever ideas naturally pop out of the algebra.

To start off, suppose without loss of generality 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. We treat the expressions as polynomials in $b$, and write

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

Since $a \leq b$, we see that either

$$0 \leq a^3 - b < a^2b < a^2b + a \quad \text{or} \quad 0 \leq b - a^3 < b < a^2b + a.$$

In any case, we have a nice term of $\frac{b}{a}$ and a bad term of $\frac{a^3 - b}{a^2b + a}$ which satisfies

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

In particular, $Q \approx \frac{b}{a}$; 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 $n \in \mathbb{Z}^+$, $r \in \mathbb{Z}$, $0 \leq r < a$. 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 $\frac{a^2 + nra + r^2 - n}{na^2 + ra + 1} = 0, 1$.  

*Crux Mathematicorum*, Vol. 43(10), December 2017
If it is 0, then note our expression is linear in \( n \) and we solve to get \( n = \frac{a^2 + r^2}{1 - ar} \). However \( n > 0 \), 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 \( \frac{a^2 + nr + r^2 - n}{n^2 + nr + r^2 + 1} = 1 \). When we multiply out, it is again linear in \( n \), and we solve to get

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

where \( a, a - r \in \mathbb{Z^+} \). In particular, we started with the pair \( (a, b) = (a, an + r) \), and found that \((a - r, a)\) gave the same quotient. If \( a = b \), we can do an easy polynomial division to check that \((1, 1)\) is the only such possibility, and it gives the quotient of \( 1 = 1^2 \). Otherwise, this decreases the sum \( a + b \), whence we can only do this finitely many times, whereupon we must be in the first case or \( a = b = 1 \).

In each case the quotient was a square, so we are done. Note that our solution also describes how to recursively find all possible positive integer pairs \((a, b)\) such that \( ab + 1 \mid a^2 + b^2 \).

### 3 A Difficult Example

Recognizing problems where the division method is applicable is normally fairly easy, as they often are similar to the example given in the previous section. However you have to keep an open mind, as there are many more problems for which it is applicable. A fantastic example is question 2 of IMO 2015:

**Problem 3:** 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.

This question was a controversial choice for the exam, and was a pain to mark. There turn out to be 4 different triples which worked (up to permutation), and thus some casework is expected. The main problem was many incomplete solutions had cases upon cases, and it was unclear if the casework would ever terminate. It was this problem where I first realized how useful the division method could be: using it we can produce a straightforward solution without mounds of endless casework.

The first question to ask is: what’s special about these numbers being powers of \( 2^2 \)? To me, the answer was that they have to divide each other. Since the expressions we are given are polynomial in nature, this seemed like quite a strong requirement.

To get started, assume that \( 0 < a \leq b \leq c \) and let

\[
ab - c = 2^x, \quad ac - b = 2^y, \quad bc - a = 2^z.
\]

Note that \( b \leq c \) implies \( b(a + 1) \leq c(a + 1) \), and thus \( ab - c \leq ac - b \). Similarly we get \( ac - b \leq bc - a \), so we have \( x \leq y \leq z \) (also \( x = y \) implies \( b = c \), and \( y = z \) implies \( a = b \)). Furthermore, \( a > 1 \) as \( a = 1 \) implies \( 2^x = b - c \leq 0 \).
Let’s eliminate $c$ by using $c = ab - 2^x$, and then our division is $ac - b \mid bc - a$, i.e.

$$2^{z - y} = \frac{bc - a}{ac - b} = \frac{ab^2 - 2^x b - a}{(a^2 - 1)b - 2^x a}$$

Now, $2^x = ab - c < ab$, so the dominant terms on the top and bottom are the $ab^2$ and $(a^2 - 1)b$ respectively; let’s bring them out. We get

$$2^{z - y} = \frac{ab}{a^2 - 1} + \frac{-2^x b - a + 2^x a^2 b}{(a^2 - 1)b - 2^x a} = \frac{ab}{a^2 - 1} + \frac{1}{a^2 - 1} \left( \frac{-a^3 + 2^x b + a}{b - 2^x a} \right),$$

and so

$$(a^2 - 1)2^{z - y} - ab = \frac{-a^3 + 2^x b + a}{(a^2 - 1)b - 2^x a} := \epsilon,$$ (1)

where $\epsilon \in \mathbb{Z}$ necessarily. This is only useful if we have a reasonable bound on $\epsilon$, which seems likely considering both $-a^3 + a$ and $2^x b$ are dominated by $a^2 b$.

Recall that the denominator of $\epsilon$ is $ac - b > 0$, hence

$$\epsilon \geq -1$$

$$\Leftrightarrow -a^3 + 2^x b + a \geq (1 - a^2)b + 2^x a$$

$$\Leftrightarrow (b - a)(a^2 + 2^x - 1) \geq 0,$$

which is true, and equality is equivalent to $a = b$ (since $a^2 + 2^x - 1 \geq a^2 > 0$). Next,

$$\epsilon \leq 1$$

$$\Leftrightarrow -a^3 + 2^x b + a \leq (a^2 - 1)b - 2^x a$$

$$\Leftrightarrow (a + b)(a^2 - 2^x - 1) \geq 0,$$

which is not as clear. If $x = 0$, this is implied by $a > 1$; otherwise $x \geq 1$ and:

$$ab \equiv c \pmod{2^x}, \quad ac \equiv b \pmod{2^x}, \quad bc \equiv a \pmod{2^x}$$

whence $b \equiv ac \equiv a^2 b \pmod{2^x}$, so $2^x \mid (a^2 - 1)b$. In particular, if $b$ is odd, then $2^x \mid a^2 - 1$, so $a > 1$ implies that $a^2 - 2^x - 1 \geq 0$. Otherwise, $b$ is even, and $a \equiv bc \equiv ab^2 \pmod{2^x}$, so $2^x \mid (b^2 - 1)a$, and thus $2^x \mid a$ since $b^2 - 1$ is odd. Now we have $a^2 - 2^x - 1 \geq 2^{2x} - 2^x - 1 \geq 2^{2x-1} - 1 \geq 1 > 0$ as desired.

To recap, we have $-1 \leq \epsilon \leq 1$, where $\epsilon = -1$ is equivalent to $a = b$, and $\epsilon = 1$ is equivalent to $a^2 = 2^x + 1$. Since $\epsilon$ was an integer, this gives three clear cases.

**Case 1**: $\epsilon = -1$. Thus $a = b$, and so $y = z$. We have $2^x = ab - c = a^2 - c$, and $2^y = ac - b = a(c - 1)$, whence $a = 2^u$, $c = 2^v + 1$ for some $u, v \in \mathbb{Z}^{\geq 0}$ with $u + v = y$. Plugging this into the first equation gives

$$2^{2u} = 2^x + 2^v + 1.$$
It is now obvious what happens when you consider binary expansions. The binary expression on the left is a single term $2^u$, whence the 3 powers of 2 on the right must combine into one, i.e. we necessarily have $x = 0, v = 1, u = 1$ or $x = 1, v = 0, u = 1$. This leads us to the solutions $(2, 2, 2)$ and $(2, 2, 3)$ (as well as permutations).

**Case 2**: $\epsilon = 0$. The equation $\epsilon = 0$ gives us $-a^3 + 2^x b + a = 0$, which implies that $b = \frac{a^3 - a}{2^x}$, so combining with equation 1 we get $2^{2-y} = \frac{ab + \epsilon}{a^2 - 1} = \frac{a^2}{2^x}$. Thus:

\[
a = 2^{\frac{x + a}{2^x}}, \quad b = \frac{a^3 - a}{2^x} = 2^{3r - x} - 2^{r - x}
\]

\[
c = ab - 2^x = 2^{4r - x} - 2^{2r - x} - 2^x
\]

\[
2^y = ac - b = 2^{5r - x} - 2^{3r - x} - 2^{x + r} - 2^{3r - x} + 2^{r - x}
\]

\[
= 2^{5r - x} - 2^{3r - x + 1} - 2^{x + r} + 2^{r - x},
\]

where $r \in \mathbb{Z}^+$ necessarily. Upon rearrangement,

\[
2^y + 2^{3r - x + 1} + 2^{x + r} = 2^{5r - x} + 2^{r - x}.
\]

Since $5r - x > r - x$, the right hand side is a valid binary representation. Since $2^{5r - x} > 2^{3r - x + 1} > 2^{r - x}$, we necessarily have $2^{3r - x + 1}$ and one of $2^y, 2^{x + r}$ must combine to give $2^{5r - x}$, with the remaining term being $2^{r - x}$. The two cases become

\[
3r - x + 1 = x + r = 5r - x - 1, \quad \text{and } y = r - x
\]

\[
3r - x + 1 = y = 5r - x - 1, \quad \text{and } x + r = r - x.
\]

We always have $3r - x + 1 = 5r - x - 1$, whence $r = 1$. The first case gives $x = \frac{3}{2}$, contradiction, and the second case gives $x = 0, y = 4$. Plugging this back in we get the valid triple $(a, b, c) = (2, 6, 11)$.

**Case 3**: $\epsilon = 1$. Equality implied $a^2 = 2^x + 1$, and from (1) we have $2^{2-y} = \frac{ab + 1}{a^2 - 1} = \frac{ab + 1}{a + 1}$. We factorize $(a - 1)(a + 1) = 2^x$, and since gcd$(a - 1, a + 1) \leq 2$, if $a - 1 \geq 2$ then one of these two factors must have a prime factor other than 2. Thus $a - 1 \leq 2$, and the only solution is $a = 3, x = 3$. So $2^{2-y} = \frac{3b + 1}{8}$ or $b = \frac{3b - 1}{8}$ with $r = x - y + 3$. From $8 = 2^x = ab - c = 3b - c$, we get $c = 3b - 8 = 2r - 9$. Finally, we plug this back into the equation for $2^y$ to get $2^y = ac - b = 3 \cdot 2^r - 27 - \frac{2r - 1}{3}$, whence

\[
3 \cdot 2^y = 2^{r+3} - 80 \Rightarrow 2^{r+3} = 2^{y+1} + 2^y + 2^6 + 2^4.
\]

This forces $y = 4, r+3 = 7$, and so $r = 4$ which gives the solution $(a, b, c) = (3, 5, 7)$.

To summarize, the only triples which work are

\[
(a, b, c) = (2, 2, 2), (2, 2, 3), (2, 6, 11), (3, 5, 7)
\]

and permutations. To get this result, we translated the power of two condition into a divisibility assertion and applied the division method. Bounding the bad term yielded 3 cases, which all reduced to equations involving sums of powers of 2, which were straightforward to solve.

Copyright © Canadian Mathematical Society, 2017
4 More Problems

For the intrepid reader, here is a short list of problems solvable with the division method:

1. (APMO 2002) Find all pairs of positive integers \((a,b)\) such that
\[
\frac{a^2 + b}{b^2 - a}, \frac{b^2 + a}{a^2 - b} \in \mathbb{Z}
\]

2. (IMO 1988 variant) 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 \(N = -5\).

3. (IMO 1998) Find all pairs of positive integers \((a,b)\) such that
\[
a^2b + b + 7 \mid ab^2 + a + b
\]

4. (Russia 2001) Find all positive integers which can be represented uniquely as
\[
\frac{x^2 + y}{xy + 1}
\]
for \(x, y\) positive integers.

5. (IMO 1994) Find all pairs of positive integers \((m,n)\) such that
\[
\frac{n^3 + 1}{mn - 1} \in \mathbb{Z}.
\]

6. (IMO 2003) Find all pairs of integers \((a,b)\) such that
\[
\frac{a^2}{2ab^2 - b^3 + 1} \in \mathbb{Z}^+.
\]

7. (IMO 2015 variant) 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 \(p\).

8. (IMO 2015 variant) 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 \((a,b,c) = (p^u,p^v,p^{2u} + 1)\) for some non-negative integer \(u\), or \(a = 1\).

---

*Crux Mathematicorum*, Vol. 43(10), December 2017