Chapter 2

Mason's Theorem

So far we have seen that the rational points on the unit circle can be described easily using the techniques of sweeping lines; except for one point, we get a bijection between the rational points on the unit circle and the rational numbers. Is it possible to do this for any algebraic curve? As a matter of fact, it is not; below we will give a few examples of curves that cannot be parametrized.

2.1 Snyder's Proof

A few years ago, the high school student (now Harvard undergraduate) Noah Snyder [*An alternate proof of Mason's theorem*, Elem. Math. **55** (2000), 93–94] came up with a 'proof from the Book' for Mason's ABC theorem. The following version of his proof is lifted from an article of Dan Bernstein.

Since $K[T]$ is a UFD, we can factor every nonzero polynomial f into irreducible factors: $f = cp_1^{a_1} \cdots p_r^{a_r}$, where the p_i are polynomials in T, and where $c \in K^\times$ is a constant. The product of the distinct prime factors of f is called the radical of f: $\operatorname{rad} f = p_1 \cdots p_r$.

We will also need two well known results:

Lemma 2.1.1. *Let R be a UFD (unique factorization domain).*

1. *If $m \mid ab$ and $\gcd(m, a) = 1$, then $m \mid b$.*
2. *If $a \mid m$, $b \mid m$ and $\gcd(a, b) = 1$, then $ab \mid m$.*

Both claims follow immediately from by looking at the prime factorizations of a, b and m.

The basic lemma in Snyder's proof is the following:

Lemma 2.1.2. *We have $\frac{f}{\operatorname{rad} f} \mid f'$.*

Proof. In fact, if $f(T) = p_1(T)^{a_1} \cdots p_r(T)^{a_r}$ is the prime factorization of f, then $\operatorname{rad} f = p_1(T) \cdots p_r(T)$ and $\frac{f}{\operatorname{rad} f} = p_1(T)^{a_1 - 1} \cdots p_r(T)^{a_r - 1}$. On the other hand,

$f'(T) = a_1 p_1(T)^{a_1-1} p_2(T)^{a_2} \cdots p_r(T)^{a_r} + p_1(T)^{a_1} \frac{d}{dx} p_2(T)^{a_2} \cdots p_r(T)^{a_r}$, hence $p_1(T)^{a_1-1} \mid f'(T)$. Similarly $p_j(T)^{a_j} \mid f'(T)$, and since the p_j are coprime, the result follows. □

We need one more trivial statement (note that $\deg 0 = -\infty$ by convention):

Lemma 2.1.3. *Assume that $f \mid g$ for polynomials $f, g \in K[T]$ with $\deg f > \deg g$. Then $g = 0$.*

In fact, $f \mid g$ implies $g = fh$ for some $h \in K[T]$. Then $\deg g = \deg f + \deg h$ is impossible if $\deg g$ is an integer; thus we necessarily have $g = h = 0$.

Now we can state Mason's theorem (also called the Mason-Stothers Theorem since it was discovered independently by Stothers (1981) and Mason (1984)):

Theorem 2.1.4. *Let K be a field and A, B, C nonzero elements of $K[T]$ with $A + B + C = 0$ and $\gcd(A, B, C) = 1$. If $\deg A \geq \deg \operatorname{rad} ABC$, then $A' = B' = C' = 0$.*

What this theorem says is that if $A + B = C$, then the number of prime factors of ABC cannot be too small (unless the derivatives of the factors are 0).

If the field K has characteristic 0, we can say more. In fact, in this case $A' = 0$ implies that A is constant (not so in characteristic p, where the polynomial T^p has derivative $pT^{p-1} = 0$). Thus if none of A, B or C are constant, then $\deg A \leq \deg \operatorname{rad} ABC - 1$, and by symmetry we have

Corollary 2.1.5. *Let K be a field of characteristic 0. If A, B, C are nonzero polynomials in $K[T]$ with $A + B + C = 0$ and $\gcd(A, B, C) = 1$, then*

$$\max\{\deg A, \deg B, \deg C\} \leq \deg \operatorname{rad} ABC - 1. \tag{2.1}$$

Note that this is best possible: if $A = 1$, $B = T^n$ and $C = 1 + T^n$, then $\operatorname{rad} ABC = T(T^n + 1)$ (note that $T^n + 1$ is squarefree since it is coprime to its derivative) and $n = \max\{\deg A, \deg B, \deg C\} = \deg \operatorname{rad} ABC - 1$.

If K has characteristic p (where p is odd), the example $(1 - T)^p + T^p = 1$ has $\operatorname{rad} ABC = T(1 - T)$ and $\max\{\deg A, \deg B, \deg C\} = p$, so the inequality (2.1) is not satisfied.

Proof of Theorem 2.1.4. First observe that $\gcd(A, B) = 1$ since any common divisor of A and B will also divide C, and this would imply $\gcd(A, B, C) \neq 1$. Similarly, $\gcd(B, C) = \gcd(C, A) = 1$.

Another ingredient is the equation

$$C'B - CB' = AB' - A'B. \tag{2.2}$$

Its proof is easy: $C'B - CB' = (-A' - B')B + (A + B)B' = AB' - A'B$.

Now let us start with the actual proof. By Lemma 2.1.2, $\frac{C}{\operatorname{rad} C}$ divides both C and C', hence their linear combination $C'B - CB'$. Similarly, $\frac{B}{\operatorname{rad} B} \mid (C'B - CB')$. Finally, (2.2) shows that $\frac{A}{\operatorname{rad} A} \mid AB' - A'B = C'B - CB'$. Since

the A, B and C are coprime, so are the quotients $\frac{A}{\operatorname{rad} A}$, $\frac{B}{\operatorname{rad} B}$ and $\frac{C}{\operatorname{rad} C}$. Thus we conclude that

$$\frac{A}{\operatorname{rad} A}\frac{B}{\operatorname{rad} B}\frac{C}{\operatorname{rad} C} \mid (C'B - CB').$$

Since A, B, C are pairwise coprime, we have $(\operatorname{rad} A)(\operatorname{rad} B)(\operatorname{rad} C) = \operatorname{rad}(ABC)$, hence

$$\frac{ABC}{\operatorname{rad}(ABC)} \mid (C'B - CB').$$

Our assumption $\deg A \geq \deg \operatorname{rad} ABC$ now implies

$$\begin{aligned}\deg \frac{ABC}{\operatorname{rad}(ABC)} &= \deg ABC - \deg \operatorname{rad} ABC \\ &\geq \deg ABC - \deg A = \deg BC \\ &> \deg(C'B - CB').\end{aligned}$$

Lemma 2.1.3 implies that $0 = C'B - CB' = AB' - A'B$. But then $A \mid A'B$, hence $A \mid A'$ since $(A, B) = 1$. Since $\deg A > \deg A'$, this implies $A' = 0$.

Similarly, $BC' = CB'$ implies $B \mid B'$, and thus we find $A' = B' = C' = 0$. □

2.2 Fermat's Last Theorem for Polynomials

As you all know, Fermat's Last Theorem states that there are no nonzero integers such that $X^n + Y^n = Z^n$ for $n > 2$. Equivalently, after dividing through by Z^n it claims that there are no nontrivial rational points on the Fermat curve $x^n + y^n = 1$.

Is Fermat's Last Theorem true for polynomials? According to Ribenboim's books, it was Liouville (not the J. Liouville famous for his theorems on elliptic functions) in 1879 who proved that it actually does hold, even for $n = 2$. I don't understand his proof, which is not too bad since we actually know a counterexample: our parametrization of the unit circle showed that

$$(1 - t^2)^2 + (2t)^2 = (1 + t^2)^2.$$

If we substitute $t = T^n$, we get

$$(1 - T^{2n})^2 + (2T^n)^2 = (1 + T^{2n})^2.$$

This is just what is allowed by Mason's theorem: we have $\deg A = 4n$ and $\deg \operatorname{rad} ABC = \deg T(1 - T^{2n})(1 + T^{2n}) = 4n + 1$.

The correct version of Fermat's Last Theorem for polynomials states

Theorem 2.2.1. *The Fermat curve $x^n + y^n + 1 = 0$ does not have a nontrivial $\mathbb{C}(t)$-rational point for $n > 2$.*

Proof. Assume that the curve can be parametrized by rational functions (i.e., quotients of polynomials). Clearing denominators we find polynomials with $X(T)^n + Y(T)^n + Z(T)^n = 0$. Hence $\deg X(T)^n \le h(XYZ) \le s-1$, where s is the number of distinct roots of XYZ. Thus $s - 1 < \deg XYZ$, and therefore $n \deg X = \deg X^n \le \deg X + \deg Y + \deg Z - 1$. The same inequality holds for Y and Z; adding them gives $n(\deg X + \deg Y + \deg Z) \le 3(\deg X + \deg Y + \deg Z) - 3$, which implies that $n < 3$. □

Note that if the Fermat curve does not have nontrivial $\mathbb{C}(t)$-rational points, then the same is true for $\mathbb{Q}(t)$-rational points.

Fermat's Last Theorem for polynomials can be proved in many different ways; Shanks, in his book *Solved and Unsolved Problems in Number Theory*, discusses a proof given by Chebyshev using integration.

Proof by descent

(This proof was not discussed in class).

Here's a proof similar to Kummer's proof of FLT (for regular prime exponents) in the integers (see N. Greenleaf, *On Fermat's equation in* $\mathbb{C}(t)$, Amer. Math. Monthly **76** (1969), 808–809): assume that there exist coprime polynomials $a, b, c \in \mathbb{C}[x]$ with $a^n + b^n = c^n$ for some $n > 2$, and pick one for which $N = \max\{\deg a, \deg b, \deg c\}$ is minimal. Since the roots of $x^n + 1$ are $-\zeta^j$ for a primitive n-th root of unity (such as $\zeta = \exp\frac{2\pi i}{n}$) and $j = 0, 1, \ldots, n-1$, we have the factorization

$$a^n + b^n = (a+b)(a+b\zeta)(a+b\zeta^2)\cdots(a+b\zeta^{n-1}).$$

We claim that these factors are relatively prime. In fact, let $d = \gcd(a+b\zeta^r, a+b\zeta^s)$; then d divides the difference $b(\zeta^r - \zeta^s)$, hence b (as $\zeta^r - \zeta^s \in \mathbb{C}$ is a unit). Moreover, d divides $\zeta^{s-r}(a+b\zeta^r) - (a+b\zeta^s) = a(\zeta^{s-r} - 1)$, i.e., $d \mid a$. Since $\gcd(a, b) = 1$ by assumption, this proves our claim.

Since c^n has factors with multiplicity divisible by n, each factor $a+b\zeta^r$ must be an n-th power:

$$a + b = f_0^n, \quad a + b\zeta = f_1^n, \quad \ldots, a + b\zeta^{n-1} = f_{n-1}^n.$$

Thus

$$a = \frac{f_1^n - \zeta f_0^n}{1-\zeta}, \quad b = \frac{f_1^n - f_0^n}{\zeta - 1},$$

hence (here we use $n > 2$)

$$f_2^n = (\zeta + 1) f_1^n - \zeta f_0^n.$$

Now put $a_1 = \sqrt[n]{\zeta+1}\, f_1$ and $b_1 = -\sqrt[n]{\zeta}\, f_0$; then (a_1, b_1, f_2) is a triple of polynomials in $\mathbb{C}[t]$ satisfying the Fermat equation of exponent n.

Now $\deg a_1 = \deg f_1 \le \frac{1}{n}\max\{\deg a, \deg b\} \le \frac{N}{n}$, and similarly $\deg b_1 \le \frac{N}{n}$ and $\deg f_2 \le \frac{N}{n}$. This contradicts the minimality of N, and the proof is complete.

Proof using algebraic geometry

The simplest proof uses concepts from algebraic geometry we have not yet talked about. A polynomial solution of the Fermat equation is a rational map from the projective line $\mathbb{P}^1\mathbb{C}$ to the Fermat curve. It is known that rational maps from the projective line to a curve exist only if the curve has genus 0. But the Fermat curve has genus $\frac{(n-1)(n-2)}{2}$, which is > 0 for $n > 2$.

Fermat's Last Theorem for the exponent 4

Just as over the integers we can prove

Proposition 2.2.2. *The equation $X^4 + Y^4 = Z^2$ has only trivial solutions in $\mathbb{C}[T]$.*

Proof. Mason's Theorem. □

This can easily be generalized:

Theorem 2.2.3. *Let $p, q, r \in \mathbb{N}$ integers. If $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} \leq 1$, then the generalized Fermat equation*

$$X^p + Y^q + Z^r = 0$$

does not have nontrivial (nonzero, not all constant) solutions in $\mathbb{C}[t]$.

Proof. Mason's theorem gives $p \cdot \deg X < \deg XYZ$; now divide through by $p \cdot \deg XYZ$: this shows that $\frac{\deg X}{\deg XYZ} < \frac{1}{p}$. Similarly, $\frac{\deg Y}{\deg XYZ} < \frac{1}{q}$ and $\frac{\deg Z}{\deg XYZ} < \frac{1}{r}$. Adding these three inequalities gives $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} > 1$. □

2.3 Elliptic Curves

An elliptic curve in Weierstrass form is a curve defined by an equation $y^2 = f(x)$, where the polynomial $f(x) = x^3 + ax^2 + bx + c$ does not have multiple roots. We will see later that the curve can be parametrized if f has multiple roots. A proof using only Mason's theorem would be more than welcome.

Proposition 2.3.1. *The elliptic curve $y^2 = x^3 + x$ cannot be parametrized.*

Proof. Write $x = \frac{m}{M}$ and $y = \frac{n}{N}$ for polynomials $m, n, M, N \in \mathbb{C}[t]$ with $(m, M) = (n, N) = 1$. Clearing denominators we get $n^2M^3 = m^3N^2 + mM^2N^2$. Clearly we have $N^2 \mid M^3$. On the other hand, $M^2 \mid m^3N^2$, hence $M \mid N$ since $(m, M) = 1$. But then $M^3 \mid N^2$, and this implies that $M^3 = cN^2$ for some unit $c \in \mathbb{C}$.

Writing N for $\sqrt{c}N$ we may assume that $M^3 = N^2$. Unique factorization shows that $M = e^2$ and $N = e^3$ for some $e \in \mathbb{C}[t]$. Thus $n^2e^6 = m^3e^6 + me^{10}$, and therefore $n^2 = m^3 + me^4 = m(m^2 + e^4)$. Since the factors on the right hand side are coprime, $m = u^2$ is a square, and we have $n^2 = u^2(u^4 + e^4)$. This in turn implies that $u^4 + e^4 = z^2$ for some $z \in \mathbb{C}[t]$, which contradicts Prop. 2.2.2. □

2.4 ABC Conjecture.

The result for integers analogous to Mason's ABC theorem is a conjecture not likely to be proved in the near future. Define $h(A,B,C) = \max\{|A|,|B|,|C|\}$ and let $\mathrm{rad}(A)$ denote the product of the disctinct prime factors of A, that is, the largest squarefree divisor of A.

ABC Conjecture. *If A, B, C are integers such that $\gcd(A,B,C) = 1$ and $A+B=C$, then for every $\varepsilon > 0$ there is a constant $\mu(\varepsilon)$ such that*

$$h(A,B,C) \leq \mu(\varepsilon) \cdot \mathrm{rad}(ABC)^{1+\varepsilon}.$$

This would be completely analogous to Mason's ABC theorem if we could choose $\varepsilon = 0$. Unfortunately, we cannot: it can be proved rather easily that the choice $\varepsilon = 0$ leads to counterexamples, no matter how large the constant μ is chosen.

For coprime natural numbers a, b, c with $a + b = c$ define

$$P(a,b,c) = \frac{\log \max\{a,b,c\}}{\log \mathrm{rad}(abc)}.$$

Then the ABC conjecture can be stated as

ABC Conjecture. For any $\eta > 1$ there are only finitely many integers a, b, c with $P(a,b,c) > \eta$.

Triples with $P > 1.4$ are called good abc triples. The current record holder is Eric Reyssat's example $A = 2$, $B = 3^{10} \cdot 109$, $C = 23^5$ with $P(A,B,C) \approx 1.62991$. Any triple with $P(A,B,C) > 1.53$ is in the current top ten.

The analogue of the Generalized Fermat Conjecture (Theorem 2.2.3) is believed to be true for integers:

Fermat-Catalan Conjecture. *If p, q, r are natural numbers with $\frac{1}{p}+\frac{1}{q}+\frac{1}{r} < 1$, then there exist only finitely many coprime integers x, y, z such that $x^p + y^q = z^r$.*

This can be deduced from the ABC conjecture. Here's the list of known solutions:

$$\begin{aligned}
1 + 2^3 &= 3^2 & 17^7 + 76271^3 &= 21063928^2 \\
2^5 + 7^2 &= 3^4 & 1414^3 + 2213459^2 &= 65^7 \\
7^3 + 13^2 &= 2^9 & 9262^3 + 15312283^2 &= 113^7 \\
2^7 + 17^3 &= 71^2 & 43^8 + 96222^3 &= 30042907^2 \\
3^5 + 11^4 &= 122^2 & 33^8 + 1549034^2 &= 15613^3
\end{aligned}$$

The first entry here is the only solution to Catalan's equation $x^p + 1 = y^q$, as was proved by Mihailescu in 2002.