Vieta in Action

Tristan Shin

26 Oct 2024

If you have any questions/comments or find any mistakes, please contact me at trshin@ucsd.edu.
This handout is linked at mathweb.ucsd.edu/~trshin/handouts/vieta_in_action.pdf.

1 Vieta's formulae

For $0 \leq k \leq n$, let

$$e_k(x_1, \ldots, x_n) \coloneqq \sum_{1 \leq i_1 < \cdots < i_k \leq n} x_{i_1} x_{i_2} \ldots x_{i_k}.$$

Theorem 1.1: Vieta's formulae

Let $a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$ be a polynomial with roots $r_1, \ldots, r_n$ (with multiplicity). Then for $0 \leq k \leq n$,

$$e_k(r_1, \ldots, r_n) = (-1)^k \frac{a_{n-k}}{a_n}.$$

2 Discussion

2.1 Symmetric polynomials

For $k \geq 1$, let

$$p_k(x_1, \ldots, x_n) \coloneqq x_1^k + x_2^k + \cdots + x_n^k.$$

Proposition 2.1: Newton's identities

For all $1 \leq k \leq n$,

$$e_k = \frac{1}{k} \sum_{i=1}^{k} (-1)^{i-1} e_{k-i} p_i.$$

Thus

$$p_k = (-1)^{k-1} k e_k + \sum_{i=1}^{k-1} (-1)^{k-1-i} e_{k-i} p_i.$$

Remark. If you extend the definition of e_k so that it is 0 for all $k > n$ (why does this make sense?), then the identity is still true.

Theorem 2.2: Fundamental theorem of symmetric polynomials

Let f be a symmetric polynomial in n variables with integer coefficients. Then f can be written uniquely in the form $g(e_1, \dots, e_n)$ for some polynomial g with integer coefficients.

2.2 Vieta jumping

Example 2.3: IMO 1988/6

Let a and b be positive integers such that $ab + 1$ divides $a^2 + b^2$. Show that

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

is the square of an integer.

Example 2.4

Characterize all rational points on the unit circle $x^2 + y^2 = 1$. Use this to characterize all Pythagorean triples.

Example 2.5

Consider the curve $y^2 = x^3 - 34x + 37$. Both $(1, 2)$ and $(6, 7)$ lie on the curve. Can you find another integer point on the curve?

Example found at https://www.umsl.edu/~siegelj/information_theory/projects/elliptic_curves_group_law.pdf

3 Problems

1. (2003 AIME II #9) Consider the polynomials $P(x) = x^6 - x^5 - x^3 - x^2 - x$ and $Q(x) = x^4 - x^3 - x^2 - 1$. Given that z_1, z_2, z_3, and z_4 are the roots of $Q(x) = 0$, find $P(z_1) + P(z_2) + P(z_3) + P(z_4)$.

2. (2023 ARML Local I7) The line through $A = (-3, -1)$ and $B = (2, 1)$ intersects the unit circle $x^2 + y^2 = 1$ at two points P and Q, with P between A and Q. Compute $AP - BQ$.

3. (2020 SDOC #16) There is a unique polynomial P with degree 8 such that $P(1/n) = 1/(n + 1)$ for $n = 1, 2, \dots, 9$. Compute the sum of the reciprocals of the roots of P (assume P has no double roots).

4. Let p be a prime and k be an integer. Compute

$$\sum_{j=1}^{p-1} j^k \pmod{p}.$$

Hint: what is a polynomial mod p that has roots $1, 2, \ldots, p-1$?

5. The **discriminant** of a monic polynomial is defined to be

$$\prod_{1 \le i < j \le n} (r_i - r_j)^2,$$

where $r_1, \ldots, r_n$ are the roots of the polynomial (with multiplicity).

   (a) What is the discriminant of $x^2 + ax + b$?

   (b) What is the discriminant of $x^3 + ax + b$?

   (c) Suppose $a_n = a_0 = 1$. What is the relationship between the discriminants of $a_n x^n + \cdots + a_1 x + a_0$ and $a_0 x^n + \cdots + a_{n-1} x + a_n$?

6. For $x_1, \ldots, x_n \in \mathbb{R}$, let

$$f(x_1, \ldots, x_n) = \sum_{j=0}^{n} c_j e_j(x_1, \ldots, x_n)$$

for some $c_j \in \mathbb{R}$. Over all $(x_1, \ldots, x_n)$ with $x_i \ge 0$ and $x_1 + \cdots + x_n = 1$, consider the set of $(x_1, \ldots, x_n)$ that minimize $f(x_1, \ldots, x_n)$. Among these, let $(y_1, \ldots, y_n)$ have the most zeros. Prove that all the nonzero y_i are equal.

7. Characterize all rational points on the circle $x^2 + y^2 = 2$. Use this to characterize all 3-term arithmetic progressions of perfect squares.

   Challenge (very hard): Can you find a 4-term arithmetic progression of perfect squares?

8. (2007 IMO #5) Let a and b be positive integers. Show that if $4ab-1$ divides $(4a^2-1)^2$, then $a = b$.

9. (Putnam) Among all tuples (a, b, c, d) of integers satisfying

$$p_2(a, b, c, d) = e_3(a, b, c, d),$$

prove that $\min\{a, b, c, d\}$ can be arbitrarily large.

10. (Crux Mathematicorum) Suppose a, b, and c are positive integers such that

$$0 < a^2 + b^2 - abc < c.$$

Show that $a^2 + b^2 - abc$ is a perfect square.

3.1 Problems about further topics

The following are problems that relate to advanced topics that you may or may not have seen before. They mostly don't require knowledge of these further topics, but rather help to build the theory for these advanced topics.

11. Let G be a graph with vertices $v_1, \ldots, v_n$. Consider the $n \times n$ matrix $A = (a_{ij})$ defined as

$$a_{ij} = \begin{cases} 1 & \text{if } v_i v_j \text{ is an edge in } G \\ 0 & \text{else} \end{cases}$$

(in particular, $a_{ii} = 0$). Let A have eigenvalues $\lambda_1, \ldots, \lambda_n$. Prove that the number of closed walks of length k in G is equal to $\lambda_1^k + \cdots + \lambda_n^k$.

Here is a guide to follow, in case you don't know much about graph theory or linear algebra:

- The **eigenvalues** of A are the values $\lambda \in \mathbb{C}$ for which there exists a nonzero vector $\mathbf{v}$ such that $A\mathbf{v} = \lambda\mathbf{v}$. There is a subtlety with repeated values of λ, but for simplicity you may assume that A has n distinct eigenvalues.
- It can be shown that the eigenvalues are precisely the solutions to $\det(A - \lambda I) = 0$, where I is the $n \times n$ identity matrix (so $A - \lambda I$ is the result of subtracting λ from each diagonal entry of A).
- A handy formula for the determinant of $A = (a_{ij})$ is

$$\det(A) = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) a_{1\sigma(1)} a_{2\sigma(2)} \ldots a_{n\sigma(n)}.$$

  Here, the sum is over all permutations σ of $\{1, \ldots, n\}$, and $\operatorname{sgn}(\sigma) = \pm 1$ depending on how many swaps it takes to "undo" σ (1 if even, -1 if odd).
- Show that the sum of the diagonal entries of A is $\lambda_1 + \cdots + \lambda_n$. (This is called the **trace** of A.)
- Now show the desired result.

12. Describe a way to generate all solutions to

$$x^2 + y^2 + z^2 = 3xyz$$

in positive integers. The numbers that appear in such solutions are called **Markov numbers**.

13. Let p be an odd prime. Suppose that $r = a + \sqrt{b}$ for integers a, b such that b is not a quadratic residue mod p. Prove that r^{p+1} can be written in the form $c + d\sqrt{b}$ for integers c, d such that p divides d.

Can you come up with a similar result for $r = a + \sqrt[3]{b}$ where b is not a cubic residue mod p?

14. This problem is not that conceptually hard, just a lot of computation. Define the symmetric polynomials

$$\begin{aligned}
s_1(x_1,\dots,x_n) &\coloneqq e_1(x_1,\dots,x_n)\\
s_{11}(x_1,\dots,x_n) &\coloneqq e_2(x_1,\dots,x_n)\\
s_2(x_1,\dots,x_n) &\coloneqq e_2(x_1,\dots,x_n)+p_2(x_1,\dots,x_n)\\
m_{111}(x_1,\dots,x_n) &\coloneqq \sum_{1\le i<j<k\le n} x_ix_jx_k = e_3(x_1,\dots,x_n)\\
m_{21}(x_1,\dots,x_n) &\coloneqq \sum_{1\le i\ne j\le n} x_i^2x_j\\
m_3(x_1,\dots,x_n) &\coloneqq \sum_{i=1}^{n} x_i^3 = p_3(x_1,\dots,x_n)\\
s_{111}(x_1,\dots,x_n) &\coloneqq m_{111}(x_1,\dots,x_n)\\
s_{21}(x_1,\dots,x_n) &\coloneqq 2m_{111}(x_1,\dots,x_n)+m_{21}(x_1,\dots,x_n)\\
s_3(x_1,\dots,x_n) &\coloneqq m_{111}(x_1,\dots,x_n)+m_{21}(x_1,\dots,x_n)+m_3(x_1,\dots,x_n).
\end{aligned}$$

(a) It turns out that every homogeneous degree-3 symmetric polynomial with integer coefficients can be written uniquely in the form $c_{111}m_{111}+c_{21}m_{21}+c_3m_3$ for some integers c_{111},c_{21},c_3. Using this, prove that the same holds for the s, i.e. every homogeneous degree-3 symmetric polynomial with integer coefficients can be written uniquely in the form $\tilde{c}_{111}s_{111}+\tilde{c}_{21}s_{21}+\tilde{c}_2s_3$ for some integers $\tilde{c}_{111},\tilde{c}_{21},\tilde{c}_3$.

(b) Both $s_{11}s_1$ and s_2s_1 are homogenous degree-3 symmetric polynomials with integer coefficients. Write them as linear combinations of s_{111},s_{21},s_3 with integer coefficients.

(c) Generalize the definitions of m to $m_{1111},m_{211},m_{22},m_{31},m_4$. Then define

$$\begin{aligned}
s_{1111} &= m_{1111}\\
s_{211} &= 3m_{1111}+m_{211}\\
s_{22} &= 2m_{1111}+m_{211}+m_{22}\\
s_{31} &= 3m_{1111}+2m_{211}+m_{22}+m_{31}\\
s_4 &= m_{1111}+m_{211}+m_{22}+m_{31}+m_4.
\end{aligned}$$

As before, we have some statement about linear combinations. All of the products $s_{111}s_1, s_{21}s_1, s_3s_1, s_2s_{11}, s_{11}^2, s_2^2$ are homogenous degree-4 symmetric polynomials. Write them as linear combinations of $m_{1111},m_{211},m_{22},m_{31},m_4$.

You can imagine generalizing this further. It turns out that the coefficients that I am using to define the s in terms of the m have combinatorial significance (**Kostka numbers**), and the coefficients that you use to write the products of two s as linear combinations of the s also have combinatorial significance (**Littlewood–Richardson coefficients**).