beforehand exactly what Euclid says in his theorem and its demonstration, we may save him some trouble by informing him that the theorem referred to in the title of M. Perott's "remark" is the twentieth proposition of the ninth book. He will find that Euclid does not say in so many words that the number of primes is infinite, but that however far the progression of primes is carried there are always more, which is equivalent to saying that the number is unlimited.

Those were the days! When editors of popular magazines actually read *The American Journal of Mathematics*! To be sure, the editor evidently was unaware of the vast development of number theory at the time, a development that made Euclid's *Elements* utterly irrelevant to the work of a contemporary mathematician specializing in this area. Although the note was anonymous, it was almost certainly written by Wendell Phillips Garrison (1840–1907), who was the literary editor of *The Nation* at the time, a man with a strong interest in science. He is the author of a book [**1**] on Darwin's voyage in the *Beagle*.

REFERENCES

1. W. P. Garrison, *What Mr. Darwin Saw in His Voyage Around the World in The Ship* Beagle. Harper, New York, 1904.
2. L. J. P. Kilford, An infinitude of proofs of the infinitude of primes (2008), available at http://arxiv.org/PS_cache/math/pdf/0610/0610066v2.pdf.
3. J. Perott, Sur l'infinité de la suite des nombres premiers, *Bulletin de la Société Mathématique et Astronomique de France* **V** (1881) 183–184.
4. ———, Remarque sur le théorème d'Euclide sur l'infinité des nombres premiers, *Amer. J. Math.* **11** (1889) 99–138. doi:10.2307/2369414
5. ———, Remarque sur le théorème d'Euclide sur l'infinité des nombres premiers, *Amer. J. Math.* **13** (1891) 235–308. doi:10.2307/2369576

Department of Mathematics, University of Vermont, Burlington, VT 05405
cooke@cems.uvm.edu

When Is a Polynomial a Composition of Other Polynomials?

James Rickards

Abstract. In this note we explore when a polynomial $f(x)$ can be expressed as a composition of other polynomials. First, we give a necessary and sufficient condition on the roots of $f(x)$. Through a clever use of symmetric functions we then show how to determine if $f(x)$ is expressible as a composition of polynomials without needing to know any of the roots of $f(x)$.

1. INTRODUCTION. The problem that sparked this paper is as follows:

Let $f(x)$ be a quadratic polynomial. Prove that there exist quadratic polynomials $g(x)$ and $h(x)$ for which

$$f(x)f(x+1) = g(h(x)) \quad [\mathbf{1}, \text{problem 683}].$$

doi:10.4169/amer.math.monthly.118.04.358

If $f(x)$ has roots r, s then $f(x+1)$ has roots $r-1, s-1$; the roots of $f(x)f(x+1)$ are $r-1, r, s-1, s$. A key observation that leads to a simple construction of $g(x)$ and $h(x)$ is that $(r-1)+s = r+(s-1)$; the sum of two roots is the same as the sum of the other two. It turns out that this is a necessary and sufficient condition for a quartic to be a composition of two quadratics. In this paper we shall prove this by way of also generalizing this result to polynomials of higher degrees. Furthermore, we shall provide an algorithm to determine if a polynomial is equal to a composition of polynomials and, if so, to find a set of compositional factors.

For a multiset $X = \{x_1, x_2, \ldots, x_n\}$ and any k such that $1 \le k \le n$, we denote by $\sigma_k(X)$ the kth symmetric function of the variables x_i, the sum of $\binom{n}{k}$ products of k of the x_i:

$$\sigma_k(X) = \sum x_{\alpha_1} x_{\alpha_2} \cdots x_{\alpha_k},$$

where the sum is taken over all k-tuples $(\alpha_1, \alpha_2, \ldots, \alpha_k)$ for which $1 \le \alpha_1 < \cdots < \alpha_k \le n$. Define $\sigma_0(X) = 1$. We recall that if $f(x) = (x-x_1)(x-x_2)\cdots(x-x_n) = x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_0$, then for all j satisfying $1 \le j \le n$, $a_{n-j} = (-1)^j \sigma_j(X)$. Also recall that if $f(x) = g(h(x))$ for polynomials f, g, and h, then the degree of f is the product of the degrees of g and h.

2. THE CRITERION FOR COMPOSITION.

Proposition 1. *Let m and n be integers exceeding one, and let R be the multiset of roots of a monic polynomial $f(x)$ of degree mn, where each root is listed as often as its multiplicity. Then $f(x)$ can be written as the composite $g(h(x))$ for monic polynomials $g(x)$ and $h(x)$ of degrees m and n respectively if and only if R can be partitioned into m multisets $S_1, S_2, \ldots, S_m$, each with n elements, such that, for each integer j with $1 \le j \le n-1$,*

$$\sigma_j(S_1) = \sigma_j(S_2) = \cdots = \sigma_j(S_m).$$

Proof. Suppose that the multiset R of roots of f can be partitioned as indicated. Let $R = \{r_1, r_2, \ldots, r_{mn}\}$ be the multiset of roots of f, each listed as often as its multiplicity and indexed so that $S_1 = \{r_1, r_2, \ldots, r_n\}$, $S_2 = \{r_{n+1}, r_{n+2}, \ldots, r_{2n}\}$, $\ldots$, $S_m = \{r_{(m-1)n+1}, r_{(m-1)n+2}, \ldots, r_{mn}\}$. For each i such that $1 \le i \le m$, let

$$y_i(x) = (x - r_{(i-1)n+1})(x - r_{(i-1)n+2}) \cdots (x - r_{in})$$

be the monic polynomial whose roots are the elements of S_i. Then, if i and j are positive integers not exceeding m, the condition that the corresponding symmetric functions of S_i and S_j are equal except for possibly the nth implies that $y_i(x) - y_j(x)$ is a constant. Define $z_i = y_1(x) - y_i(x)$ for each i with $1 \le i \le m$.

Let $h(x) = y_1(x)$ and

$$g(x) = (x - z_1)(x - z_2) \cdots (x - z_m).$$

Then

$$\begin{aligned} g(h(x)) &= (y_1(x) - z_1)(y_1(x) - z_2) \cdots (y_1(x) - z_m) = y_1(x) y_2(x) \cdots y_m(x) \\ &= \prod_{i=1}^{mn} (x - r_i) = f(x). \end{aligned}$$

Now we prove that the condition on the roots of f is necessary. Suppose that we are given monic polynomials g and h of respective degrees m and n for which $f(x) = g(h(x))$. Let

$$g(x) = (x - t_1)(x - t_2) \cdots (x - t_m).$$

For each positive integer i not exceeding m, let

$$u_i(x) = h(x) - t_i = (x - r_{(i-1)n+1})(x - r_{(i-1)n+2}) \cdots (x - r_{in}),$$

say, where each linear factor is listed as often as the multiplicity of the corresponding root of u_i. Then

$$\begin{aligned} f(x) = g(h(x)) &= (h(x) - t_1)(h(x) - t_2) \cdots (h(x) - t_m) \\ &= (x - r_1)(x - r_2) \cdots (x - r_{mn}), \end{aligned}$$

so that the r_j are the roots of f.

For each index i with $1 \le i \le m$, $u_i(x) = h(x) - t_i$, so that all the coefficients of u_i except the constant are independent of i. It follows that all the symmetric functions of the roots of the polynomials u_i agree except perhaps the nth. Thus, we obtain the desired partition, where S_i consists of the roots of u_i. Note that in our partition of the roots, $\sigma_j(S_i)$ is $(-1)^j$ times the coefficient of x^{n-j} in $h(x)$ for $0 \le j \le n - 1$ and $1 \le i \le m$. ∎

Let us deal with polynomials in general.

Proposition 2. *Suppose that $f(x)$ is a polynomial of degree mn and leading coefficient a, so that $f(x) = au(x)$ for some monic polynomial $u(x)$. Then $f(x)$ is a composite of polynomials of degrees m and n if and only if $u(x)$ is a composite of monic polynomials of degrees m and n.*

Proof. Suppose that $f(x) = g(h(x))$, where $g(x)$ is of degree m with leading coefficient b and $h(x)$ is of degree n with leading coefficient c. Then, by comparison of leading coefficients, we have that $a = bc^m$. It can be checked that $u(x) = v(w(x))$ where $v(x) = (bc^m)^{-1} g(cx)$ and $w(x) = c^{-1}h(x)$. It is also easily seen that $v(x)$ and $w(x)$ are both monic.

On the other hand, suppose that $u(x) = v(w(x))$ for some monic polynomials $v(x)$ and $w(x)$ of respective degrees m and n. Then $f(x) = g(h(x))$ with $g(x) = av(x)$ and $h(x) = w(x)$. ∎

We note that, even for monic polynomials, the decomposition of $f(x)$ as a composite $g(h(x))$ is not unique. For example, for arbitrary values of a and d, the pairs $(g(x), h(x)) = (x^2 + d, x^2 + ax + 1)$ and $(g(x), h(x)) = (x^2 + 2x + d + 1, x^2 + ax)$ both yield

$$f(x) = x^4 + 2ax^3 + (a^2 + 2)x^2 + 2ax + 1 + d = (x^2 + ax + 1)^2 + d.$$

However, as one might expect from the involvement of a particular partition of the roots of $f(x)$, the different pairs $(g(x), h(x))$ are closely linked.

Proposition 3. *Let m and n be integers exceeding one. Then there are polynomials $p_1, p_2, \ldots, p_{n-1}$ (where for each i, p_i is a function of i variables) such that for any monic polynomials $f(x)$, $g(x)$, and $h(x)$ of degrees mn, m, and n respectively, if*

$f(x) = g(h(x)) = x^{mn} + a_{mn-1}x^{mn-1} + \cdots + a_0$, *and* $h(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_0$, *then we have* $c_{n-j} = p_j(a_{mn-1}, a_{mn-2}, \ldots, a_{mn-j})$ *for all* j *such that* $1 \le j \le n-1$.

Proof. The coefficient of x^n in $h(x)$ is 1, so let $c_n = 1$. As in Proposition 1, let R be the multiset of roots of $f(x)$, and $S_1, S_2, \ldots, S_m$ be the partition of roots constructed in Proposition 1. We observed that for our partition of the roots of $f(x)$, $\sigma_j(S_i) = (-1)^j c_{n-j}$ for $1 \le i \le m$ and $0 \le j \le n-1$. Equating expressions for the sum of roots of $f(x)$, we find that

$$a_{mn-1} = -\sigma_1(R) = -\sum_{i=1}^{m} \sigma_1(S_i) = mc_{n-1},$$

so $c_{n-1} = p_1(a_{mn-1})$, where $p_1(x_1) = x_1/m$. We now construct the polynomials p_i for $2 \le i \le n-1$ recursively. The expression $\sigma_k(R)$ with $2 \le k \le n-1$ consists of $\binom{mn}{k}$ terms, each the product of k roots in R. Some of these terms will have all their factors drawn from exactly one of the S_i; the sum of all such terms is $\sum_{i=1}^{m} \sigma_k(S_i) = (-1)^k mc_{n-k}$. The remaining terms will have factors drawn from at least two of the S_i; the sum of these terms is

$$S = \sum \sigma_{b_1}(S_1)\sigma_{b_2}(S_2)\sigma_{b_3}(S_3)\cdots\sigma_{b_m}(S_m) = (-1)^k \sum c_{n-b_1}c_{n-b_2}\cdots c_{n-b_m},$$

where the summation is taken over all m-tuples $(b_1, b_2, \ldots, b_m)$ of nonnegative integers for which $0 \le b_1, b_2, \ldots, b_m \le k-1$ and $b_1 + b_2 + \cdots + b_m = k$. Thus $a_{mn-k} = (-1)^k \sigma_k(R) = mc_{n-k} + (-1)^k S$, so therefore

$$c_{n-k} = \frac{1}{m}\left(a_{mn-k} - \sum c_{n-b_1}c_{n-b_2}\cdots c_{n-b_m}\right).$$

We have already constructed polynomials $p_1, p_2, \ldots, p_{k-1}$, so we can conclude that $c_{n-k} = p_k(a_{mn-1}, a_{mn-2}, \ldots, a_{mn-k})$, where

$$p_k(x_1, x_2, \ldots, x_k) = \frac{1}{m}\left(x_k - \sum p_{b_1}(x_1, \ldots, x_{b_1})\cdots p_{b_m}(x_1, \ldots, x_{b_m})\right)$$

and the summation is taken over all m-tuples $(b_1, b_2, \ldots, b_m)$ of nonnegative integers for which $0 \le b_1, b_2, \ldots, b_m \le k-1$ and $b_1 + b_2 + \cdots + b_m = k$ (when $b_i = 0$ say $p_{b_i}(x_1, x_2, \ldots, x_{b_i}) = 1$). ∎

Proposition 3 is a very strong proposition. If there exists a suitable partition of the roots of f, then the coefficients of $h(x)$ except for the constant are uniquely determined and can be computed using only the coefficients of f; no knowledge of the roots of f is required. In fact, even if we had access to the roots of f, when the degree of f gets large we would have many different partitions of the roots to check and it may take a while to find a suitable partition (if one exists). Using Proposition 3 we exploit the fact that the coefficients of $f(x)$ are symmetric functions of its roots to easily calculate the coefficients of $h(x)$ except for the constant. This method is much more effective than if we used Proposition 1 directly to calculate $h(x)$.

3. CAN $f(x)$ BE EXPRESSED AS A COMPOSITION OF POLYNOMIALS? Suppose that $f(x)$ is a monic polynomial of degree mn, and we want to try to find monic polynomials $g(x)$ and $h(x)$ of degrees m and n, respectively, such that $f(x) = g(h(x))$. Proposition 3 allows us to identify all but the constant coefficient of $h(x)$; assign the value 0 to the constant coefficient. Write out the values of $h(x)^m$, $h(x)^{m-1}$, $\ldots$, $h(x)$, noting that the respective degrees of these polynomials are mn, $mn-n$, $\ldots$,

n. Place the coefficient 1 in front $h(x)^m$. Select e_{m-1} so that the coefficient of x^{mn-n} in $h(x)^m + e_{m-1}h(x)^{m-1}$ agrees with the coefficient of x^{mn-n} in $f(x)$. Next, select e_{m-2} so that the coefficient of x^{mn-2n} in $h(x) + e_{m-1}h(x)^{m-1} + e_{m-2}h(x)^{m-2}$ agrees with the coefficient of x^{mn-2n} in $f(x)$. Repeat the procedure to obtain numbers e_{m-1}, e_{m-2}, e_{m-3}, ..., e_1, e_0 and let $g(x) = x^m + e_{m-1}x^{m-1} + e_{m-2}x^{m-2} + \cdots + e_1x + e_0$. If $g(h(x)) = f(x)$, then we have obtained a desired representation.

But what if $g(h(x))$ is unequal to $f(x)$? May it still be possible for $f(x)$ to be represented as a composite? We show that the answer is *no*.

Suppose that $f(x) = g_1(h_1(x))$ for some polynomials g_1 and h_1 of respective degrees m and n. By Proposition 3, the coefficients of $h(x)$ and $h_1(x)$ are the same except for the constant coefficient. Hence $h(x) = h_1(x) + p$ for some constant p. Let the roots of $g_1(x)$ be $q_1, q_2, \ldots, q_m$, so that

$$f(x) = (h_1(x) - q_1)(h_1(x) - q_2)\cdots(h_1(x) - q_m).$$

Define

$$g_2(x) = (x - p - q_1)(x - p - q_2)\cdots(x - p - q_m).$$

Then

$$\begin{aligned} g_2(h(x)) &= (h(x) - p - q_1)(h(x) - p - q_2)\cdots(h(x) - p - q_m) \\ &= (h_1(x) - q_1)(h_1(x) - q_2)\cdots(h_1(x) - q_m) = f(x). \end{aligned}$$

We know that if $f(x) = g(h(x))$ for some polynomial $g(x)$, then indeed it must be the polynomial produced in the foregoing test. Thus $g(x) = g_2(x)$ and $f(x) = g(h(x))$, yielding a contradiction. Thus $f(x)$ is not equal to a composite as indicated.

The process can be extended to determining $f(x)$ as a composite of any number of compositional factors, $f(x) = f_1(f_2(f_3(\cdots(f_c(x))\cdots)))$, where the degree of f is the product of the assigned respective degrees d_i of the f_i. It will work whenever such a representation exists. We know this to be true when $c = 2$. Suppose that it is true for $c - 1$ compositional factors. Then if $f(x) = g(h(x))$ when $h(x)$ is a composite of $c - 1$ compositional factors, the process will produce a representation $f(x) = f_1(h(x) + e)$ for some constant e. Since $h(x)$ is a composite of $c - 1$ polynomials, then so is $h(x) + e$; just add the constant e to the outside polynomial. We now can apply the induction hypothesis.

4. EXAMPLES. We consider two examples to show what happens when the representation as a composite is and is not possible.

Example 1. Can

$$f(x) = x^8 + 4x^7 + 10x^6 + 16x^5 + 18x^4 + 14x^3 + 7x^2 + 2x + 3$$

be written as a composite of three quadratics? First, we try to make $f(x) = g(h(x))$, with $g(x)$ a quadratic and $h(x)$ a quartic. We have $m = 2$ and $n = 4$, so

$$\begin{aligned} p_1(x_1) &= \frac{x_1}{2}, \\ p_2(x_1, x_2) &= \frac{1}{2}\left(x_2 - (p_1(x_1))^2\right) = \frac{x_2}{2} - \frac{x_1^2}{8}, \\ p_3(x_1, x_2, x_3) &= \frac{1}{2}\left(x_3 - 2p_1(x_1)p_2(x_1, x_2)\right) = \frac{x_3}{2} - \frac{x_1x_2}{4} + \frac{x_1^3}{16}. \end{aligned}$$

Thus the coefficients of x^3, x^2, and x in $h(x)$ must be $p_1(4) = 2$, $p_2(4, 10) = 3$, and $p_3(4, 10, 16) = 2$, respectively. Therefore

$$h(x) = x^4 + 2x^3 + 3x^2 + 2x$$

and

$$(h(x))^2 = x^8 + 4x^7 + 10x^6 + 16x^5 + 17x^4 + 12x^3 + 4x^2;$$

this means that $e_1 = 1$ and $e_0 = 3$. Then

$$\begin{aligned}(h(x))^2 + h(x) + 3 &= x^8 + 4x^7 + 10x^6 + 16x^5 + 18x^4 + 14x^3 + 7x^2 + 2x + 3 \\ &= f(x),\end{aligned}$$

so that the polynomials $g(x) = x^2 + x + 3$ and $h(x) = x^4 + 2x^3 + 3x^2 + 2x$ work.

Now we try to express $h(x)$ as a composite $u(v(x))$ of two quadratics. In this case, $m = n = 2$, so

$$p_1(x_1) = \frac{x_1}{2}$$

and the coefficient of x in $v(x)$ is $p_1(2) = 1$. Thus $v(x) = x^2 + x$ and $(v(x))^2 = x^4 + 2x^3 + x^2$. Since $e_1 = 2$ and $e_0 = 0$, we try $u(x) = x^2 + 2x$. Indeed

$$u(v(x)) = (x^4 + 2x^3 + x^2) + 2(x^2 + x) + 0 = h(x),$$

with the final result that $f(x) = g(u(v(x)))$.

Example 2. Can $x^4 - 7x^3 + 14x^2 - 8x$ be expressed as a composite of two quadratics g and h? In this case, $m = n = 2$, so

$$p_1(x_1) = \frac{x_1}{2}.$$

Thus the coefficient of x in $h(x)$ is $p_1(-7) = -3.5$, so $h(x) = x^2 - 3.5x$ and $(h(x))^2 = x^4 - 7x^3 + 12.25x^2$. This leads to $e_1 = 1.75$ and $e_0 = 0$. But then

$$(h(x))^2 + 1.75h(x) + 0 = x^4 - 7x^3 + 14x^2 - 6.125x \neq f(x)$$

and we conclude that $f(x)$ cannot be expressed as a composite of two quadratics.

ACKNOWLEDGMENTS. I would like to thank Dr. Ed Barbeau from the University of Toronto for providing the problem that inspired this paper in his Mathematical Olympiads Correspondence Program and also for editing this paper. I would also like to thank Dr. Barry Jessup and Dr. Pieter Hofstra, both from the University of Ottawa.

REFERENCE

1. E. Barbeau, Mathematical olympiads correspondence program problems for May 2010, available at http://www.math.toronto.edu/barbeau/olymon99.pdf.

6300 Elkwood Drive, Greely, ON, K4P 1M9
jamesarickards@hotmail.com