Urgent - requires immediate attention

Dear [Name],

I enclose a proof copy of your contribution to the March 2013 issue of The Mathematical Gazette. It has already been checked once by our proof-readers, and some minor rewordings, punctuation changes, etc. may have been made. Please check it carefully for errors, paying special attention to the diagrams, mathematical expressions, quotations from other sources and your name and address. If you have any essential changes, please mark them in the margin of your proof copy and return it to me immediately.

Please note that your contribution is due to be included in the March 2013 issue of The Mathematical Gazette. You must return this proof copy to me no later than Thursday, January 11, 2013. I will assume that you accept the article as it stands and that you agree to the terms of publication described in the paragraph above.

If you have any queries or concerns, please contact me immediately. I may be able to accommodate some changes, but I cannot guarantee that all requests will be fulfilled.

Yours sincerely,

Gerry Leversha

---

The Mathematical Gazette
Editor: Gerry Leversha
15 Maunder Road, Hanwell, London W7 3PN
United Kingdom
Email: g.leversha@btinternet.com

Telephone (0116) 221 0013
Fax (0116) 212 2835
Registered Charity No. 313281

Copyright © The Mathematical Association 2013.
Introduction

The motivation to write this paper arose out of the following problem which was posed in a recent mathematical olympiad:

Given a polynomial with integer coefficients, show that there exist non-zero polynomials, with integer coefficients, such that

\[ P(X) = (\alpha X - \beta) \cdot Q(X) \]

where \( \alpha \) and \( \beta \) are integers.

For instance, if \( P(X) = X^2 + 3X + 2 \), then we notice that

\[ P(X) = (X - 1) \cdot (X + 2) \]

A moment's thought makes it fairly evident that this trick easily solves the first part of the problem for a general polynomial. For example, since \( f(X) \) is a polynomial of degree two, we can write \( f(X) = (\alpha X^2 - \beta X + \gamma) \) where \( \alpha, \beta, \gamma \) are integers.

What about the second part, or more generally, does the assertion hold good if we replace \( X \) by any \( X \)? By a suitable choice of \( \alpha \) and \( \beta \), we obtain the assertion. Here are the details.

Theorem

For any polynomial \( f(X) \) of degree two, there exist non-zero polynomials \( P(X) \) and \( Q(X) \) such that

\[ f(X) = (\alpha X^2 - \beta X + \gamma) \cdot Q(X) \]

where \( \alpha, \beta, \gamma \) are integers.

Proof

Let \( f(X) = aX^2 + bX + c \). Then

\[ f(X) = (\alpha X^2 - \beta X + \gamma) \cdot Q(X) \]

where \( \alpha, \beta, \gamma \) are integers.

The original problem for \( f(X) \) can be reduced to the following:

**Theorem**

For any polynomial \( f(X) \) of degree two, there exist non-zero polynomials \( P(X) \) and \( Q(X) \) such that

\[ f(X) = (\alpha X^2 - \beta X + \gamma) \cdot Q(X) \]

where \( \alpha, \beta, \gamma \) are integers.

**Proof**

Let \( f(X) = aX^2 + bX + c \). Then

\[ f(X) = (\alpha X^2 - \beta X + \gamma) \cdot Q(X) \]

where \( \alpha, \beta, \gamma \) are integers.

**Theorem**

For any polynomial \( f(X) \) of degree two, there exist non-zero polynomials \( P(X) \) and \( Q(X) \) such that

\[ f(X) = (\alpha X^2 - \beta X + \gamma) \cdot Q(X) \]

where \( \alpha, \beta, \gamma \) are integers.

**Proof**

Let \( f(X) = aX^2 + bX + c \). Then

\[ f(X) = (\alpha X^2 - \beta X + \gamma) \cdot Q(X) \]

where \( \alpha, \beta, \gamma \) are integers.

**Theorem**

For any polynomial \( f(X) \) of degree two, there exist non-zero polynomials \( P(X) \) and \( Q(X) \) such that

\[ f(X) = (\alpha X^2 - \beta X + \gamma) \cdot Q(X) \]

where \( \alpha, \beta, \gamma \) are integers.

**Proof**

Let \( f(X) = aX^2 + bX + c \). Then

\[ f(X) = (\alpha X^2 - \beta X + \gamma) \cdot Q(X) \]

where \( \alpha, \beta, \gamma \) are integers.
The composition of polynomials is given by

\[ P(X) = \sum_{n=0}^{\infty} a_n X^n \]

where \( a_n \) are the coefficients of the polynomial. 

For certain polynomials with integer coefficients, \( f(X) \) and \( g(X) \), we have

\[ Q(X) = P(-X) = f(X^2) + Xg(X^2) \]

This answers the first part.

One may adopt a similar approach for the second part. Let \( P(X) = P_0(X) + XP_1(X) + X^2P_2(X) \), and consider the cubic roots of unity. If \( \omega = 1, \omega, \omega^2 \), then

\[ Q_1(X) = P_0(X) + \omega XP_1(X) + \omega^2 X^2P_2(X) \]

and

\[ Q_2(X) = P_0(X) + \omega^2 XP_1(X) + \omega X^2P_2(X) \]

Using the identity

\[ l^3 + m^3 + n^3 - 3lmn = \sum_{i=0}^{2}(\omega^i + \omega^{i+1} + \omega^{i+2}) = 0 \]

for \( \omega = e^{2\pi i/3} \), we have

\[ P_0(X^3) + XP_1(X^3) + X^2P_2(X^3) = (X) \]

which is a polynomial with integer coefficients.

The above elementary argument indicates that the case of \( X^k \) for general \( k \) may be cumbersome to approach in this fashion. In this section, we give an elementary proof for the case \( k = 3 \) which is different from the above.
The one above for. Following that, we give another less elementary proof for the same and show in the next section that this argument carries over to show, for any non-constant polynomial in one variable over the integers and for a given polynomial with integer coefficients, there exist non-zero polynomials with integer coefficients such that \( k = P(x) = Q(x) = R(x) \).

**Lemma 1:** Let be a positive integer. Then, for each polynomial with integer coefficients, there exist non-zero with integer coefficients such that. One has an analogous statement where coefficients are allowed to be rational numbers instead of the integers.

It suffices to prove the version for polynomials over the rational numbers for, if has integer coefficients and, if we get with rational coefficients satisfying, then we may multiply out by a suitable integer to get corresponding integral polynomials.

We first give a linear algebraic proof which is illustrated by the following example.

**Example:** Let and suppose we wish to find a non-zero with integer coefficients such that  is of the form . Suppose we try to find rational so that

\[
\begin{align*}
&b_0 + b_1x + b_2x^2 + b_3x^3 + b_4x^4 + b_5x^5 + b_6x^6 = 0, \\
&b_1 + b_4x + b_5x^2 + b_6x^3 = 0, \\
&b_2 + b_3x + b_4x^2 + b_5x^3 = 0, \\
&b_3 + b_2x + b_3x^2 + b_4x^3 = 0, \\
&b_4 + b_3x + b_2x^2 + b_3x^3 = 0, \\
&b_5 + b_4x + b_3x^2 + b_2x^3 = 0, \\
&b_6 + b_5x + b_4x^2 + b_3x^3 = 0.
\end{align*}
\]

These conditions become the following linear equations for the :

\[
\begin{align*}
&b_6 = 0, \\
&b_5 = 0, \\
&b_4 = 1, \\
&b_3 = -7, \\
&b_2 = 48 + b_1, \\
&b_1 = 0, \\
&b_0 = q.
\end{align*}
\]

Put; then,. Hence, which gives , . Therefore,

\[
\begin{align*}
&b_1 = -7, \\
&b_2 = 1, \\
&b_3 = 48, \\
&b_4 = 0, \\
&b_5 = 0, \\
&b_6 = q.
\end{align*}
\]
The problem of solving linear equations in finite fields is of great importance in modern algebra and number theory. A recent paper discusses the application of finite field theory to the study of certain algebraic varieties, demonstrating how the properties of finite fields can be used to prove results in algebraic geometry. The authors also explore the relationship between finite fields and coding theory, showing how the algebraic structure of finite fields can be exploited in the design of efficient error-correcting codes. This work has implications for both theoretical and applied mathematics, and it is likely to be of interest to researchers working in a variety of fields.
Let $\mathbb{K}$ be a field; then a subset $S$ is said to be a constant field if there is an element $y$ such that $y = 0$. If a polynomial is not the zero polynomial, then there exist non-zero $a_i$ for which $(f_i) \neq 0$.

Finally, we observe that $\alpha$ is not the zero polynomial since $\alpha$ is not rational as well. As $\alpha$ is a polynomial for each $\alpha$, the monomials $\alpha^i$ and the elementary symmetric functions in the $\alpha$'s are polynomials.

The following is a multi-variable generalisation of a result in the field of polynomials.

Theorem. Let $\mathbb{K}$ be a field and $f \in \mathbb{K}[X]$. Suppose $\mathbb{K} \subseteq \mathbb{R}$.

There exist non-zero $\alpha_i$ such that $\prod \alpha_i X = d \neq 0$ if $f$ is not the zero polynomial.

Proof. As before, we may consider the polynomials over $\mathbb{Z}$.

The above second proof carries over to a general in place of $\mathbb{Z}$. (The results are in place of $\mathbb{Z}$.)