

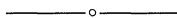
powers of the generator  $g$ , and so their product  $(-1)(-2) = 2$  must be an even power of  $g$ . In any case, we may select at least one of the quadratic factors  $(x^2 + 1)$ ,  $(x^2 + 2)$ , or  $(x^2 - 2)$  having the form  $(x^2 - g^{2e}) \bmod p$ . Let's say  $(x^2 + d)$  has  $x_0 = g^e$  as a root mod  $p$ , and suppose that  $p^b \mid (x_0^2 + d)$  so that  $x_0^2 + d = p^b c$ . Now  $2x_0$  is invertible mod  $p$ , so we may set  $x_1 = x_0 - c(2x_0)^{-1}p^b$ . Expansion reveals that

$$\begin{aligned} x_1^2 + d &= x_0^2 - 2x_0 c(2x_0)^{-1}p^b + c^2(2x_0)^{-2}p^{2b} + d \\ &\equiv p^b c - p^b c \equiv 0 \bmod p^{b+1}. \end{aligned}$$

Repeat this device to increase the exponent until we construct a root mod  $p^a$ .

Combining the roots constructed for prime powers with the Chinese Remainder Theorem gives us the required root for  $f(x) \bmod m$  for each  $m$ , in spite of the fact that  $f(x)$  has no integer root.

**Question:** Is there an example of a polynomial with these properties having degree less than 9?



### On a Theorem of Clay

H. Azad (hassanaz@kfupm.edu.sa) and A. Laradji (alaradji@dpc.klupm.edu.sa),  
King Fahd University of Petroleum and Minerals, Dhahran, Saudi Arabia

In [1], Clay proved the surprising theorem that the multiplicative group  $\mathbb{C}^*$  is isomorphic to its subgroup  $\mathbb{S}^1$ , the unit circle. His proof relies on a deep structure theorem of divisible abelian groups that can be found in [3] and in [5]. Clay's result is cited (without proof) in some standard undergraduate texts (e.g. Gallian [4, p. 121] and Nicholson [6, p. 148]). In this short note we give a much more accessible and very elementary proof of this result, showing in particular that it may well be set as an undergraduate exercise. For any set  $I$ ,  $|I|$  will denote the cardinality of  $I$ . For basic results on cardinal arithmetic we refer to any introductory text in set theory ([2], for example).

**Proposition.** *There exists a group isomorphism  $f: (\mathbb{R}, +) \rightarrow (\mathbb{C}, +)$  that extends the identity map of  $\mathbb{Q}$ .*

*Proof.* Extend  $\{1\}$  to a basis  $\mathcal{B}$  of  $\mathbb{R}$  and a basis  $\mathcal{C}$  of  $\mathbb{C}$  as  $\mathbb{Q}$ -vector spaces. We have  $|\mathbb{R}| = |\mathbb{Q}| \cdot |\mathcal{B}|$ , and therefore, since  $|\mathbb{Q}| < |\mathbb{R}|$  and  $|\mathbb{Q}| \cdot |\mathcal{B}| = \max(|\mathbb{Q}|, |\mathcal{B}|)$ , we obtain  $|\mathcal{B}| = |\mathbb{R}|$ . Similarly  $|\mathbb{C}| = |\mathbb{Q}| \cdot |\mathcal{C}|$ , and so  $|\mathbb{C}| = |\mathcal{C}|$ . Now  $|\mathbb{C}| = |\mathbb{R}^2| = |\mathbb{R}|$  (for any infinite cardinal  $\alpha$ ,  $\alpha^2 = \alpha$ ), and hence  $|\mathcal{B}| = |\mathcal{C}|$ . Choose a bijection  $g: \mathcal{B} \rightarrow \mathcal{C}$  such that  $g(1) = 1$  and extend it to a  $\mathbb{Q}$ -isomorphism  $f: \mathbb{R} \rightarrow \mathbb{C}$ . Clearly  $f$  is a group isomorphism such that  $f(q) = q$ ,  $\forall q \in \mathbb{Q}$ .

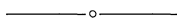
**Remark.** It is perhaps worth mentioning that the axiom of choice needed for the theory of divisible abelian groups used in [1], is again required here, but at a clearly less sophisticated level, for example for the existence of the Hamel basis above.

**Corollary.** *The multiplicative group  $\mathbb{C}^*$  is isomorphic to  $\mathbb{S}^1$ .*

*Proof.* Using the maps  $z \mapsto e^{2\pi iz} (z \in \mathbb{C})$  and  $r \mapsto e^{2\pi ir} (r \in \mathbb{R})$ , it is clear that  $\mathbb{C}^* \cong \mathbb{C}/\mathbb{Z}$  and  $\mathbb{S}^1 \cong \mathbb{R}/\mathbb{Z}$ . On the other hand the map  $f$  in the proof above maps  $\mathbb{Q}$  onto  $\mathbb{Q}$ , and hence  $\mathbb{Z}$  onto  $\mathbb{Z}$ . This induces an isomorphism  $\mathbb{C}/\mathbb{Z} \cong \mathbb{R}/\mathbb{Z}$ , as required.

## References

1. J. R. Clay, The punctured plane is isomorphic to the unit circle, *J. Number Theory* 1 (1964) 500–501.
2. H. B. Enderton, *Elements of Set Theory*, Academic Press, 1977.
3. L. Fuchs, *Infinite Abelian Groups I*, Academic Press, 1970.
4. J. A. Gallian, *Contemporary Abstract Algebra*, 4th edition, Houghton Mifflin, 1998.
5. I. Kaplansky, *Infinite Abelian Groups*, Revised edition, University of Michigan Press, 1971.
6. W. K. Nicholson, *Introduction to Abstract Algebra*, PWS Publishing, 1993.



## Tangents without Calculus

Jorge Aarão (jaarao@benson.mckenna.edu),  
Claremont McKenna College, Claremont, CA 91711

In pre-calculus courses we often teach our students about polynomial division, and use the division algorithm in factoring polynomials. I would like to suggest another interesting application of polynomial division.

Here's the no-calculus rule for finding tangent lines to polynomials.

The line  $y = mx + b$  is tangent to the graph of the polynomial  $p(x)$  at  $x = a$  if and only if  $mx + b$  is the remainder of the quotient  $p(x)/(x - a)^2$ .

For example, since

$$x^3 - 2x^2 + x + 1 = (x + 2)(x - 2)^2 + (5x - 7),$$

$y = 5x - 7$  is tangent to  $y = x^3 - 2x^2 + x + 1$  at  $x = 2$ .

While this rule may not be as simple as the calculus method for finding tangent lines, from a pre-calculus point of view it is not only elementary but also has a very intuitive, geometric justification.

First let's answer the question: when is the  $x$ -axis tangent to the graph of a polynomial? Let  $f(x)$  be a polynomial and let  $x = a$  be a root of  $f$ , then, as suggested by Figure 1, the  $x$ -axis is tangent to the graph of  $f$  exactly when  $x = a$  is (at least) a double root of  $f$ . Equivalently,  $(x - a)^2$  divides  $f(x)$  without remainder.

The question of whether a line  $y = mx + b$  is tangent to the graph of a polynomial  $p(x)$  at  $x = a$  can be reduced to the previous case by setting  $f(x) = p(x) - (mx + b)$ . Now  $y = mx + b$  is tangent to  $y = p(x)$  at  $x = a$

- $\Leftrightarrow$  the  $x$ -axis is tangent to  $y = f(x)$  at  $x = a$
- $\Leftrightarrow (x - a)^2$  divides  $f(x)$  without remainder
- $\Leftrightarrow mx + b$  is the remainder of the quotient  $p(x)/(x - a)^2$ .