P 78. Prove that a field is formally real if and only if -1 is not a sum of fourth powers.

I. G. Connell, McGill University

SOLUTIONS

P 64. Find all solutions of

$$\tan^{-1} 1 + \tan^{-1} 2 + \ldots + \tan^{-1} n = \frac{k\pi}{2} .$$

Leo Moser, University of Alberta

(A partial solution was published in vol. 6, no. 3.)

Solution by Robert Breusch, Amherst College.

If $\prod_{s=1}^{n} (1+is) = a + ib$, then a and b are clearly integers. Since $\prod_{s=1}^{n} (1+is) = \prod_{s=1}^{n} (1+s^2)^{1/2} \cdot \exp(i. \sum_{s=1}^{n} \tan^{-1} s)$, the given condition implies that $\prod_{s=1}^{n} (1+is)$ is either real, or purely imaginary, and in any case that its absolute value is an integer. It follows that $R = \prod_{s=1}^{n} (1+s^2)$ is a square, and thus that R contains each one of its distinct prime factors at least twice. Any prime whose square divides one of the factors of R, must be $\leq n$, and any prime which divides two distinct factors, $1 + s_1^2$ and $1 + s_2^2$, must divide either $s_1 - s_2$ or $s_1 + s_2$, and thus must be $\leq 2n$. It follows:

(1) R contains no primes $> 2n$.

https://doi.org/10.1017/S0008439500026801 Published online by Cambridge University Press

Let p represent primes $\equiv 1 \pmod 4$, and q primes $\equiv 3 \pmod 4$. To every p, and to every positive integer t, there exists precisely one integer s, such that $(t-1)(p/2) < s < t(p/2)$ and $s^2 \equiv -1 \pmod p$. Thus, among the n factors of R, there will be $[n/(p/2)] + \theta_{2n}(p)$ divisible by p, where $\theta_{2n}(p)$, like all the following θ's, is 0 or 1. Of these, $[2n/p^2] + \theta_{2n}(p^2)$ will be divisible by p^2, etc. Thus the total multiplicity of p in R will be

$$\sum_r [2n/p^r] + \sum_r \theta_{2n}(p^r),$$

with r such that $p^r \leq n^2 + 1 < (2n)^2$. Calling the second sum for the moment σ, we see that $p^\sigma < (2n)^2$. Since R contains the factor 2 precisely $[(n+1)/2]$ times, it follows from (1), with

$$a_{2n}(v) = \sum_r [2n/v^r],$$

that

$$R < 2^{(n+1)/2} \cdot \prod_{p \leq 2n} p^{a_{2n}(p)} \cdot (2n)^{2 \cdot \pi_1(2n)}, \tag{2}$$

where $\pi_i(2n)$ $(i = 1 \text{ or } 3)$ stands for the number of primes $\leq 2n$ and $\equiv i \pmod 4$; thus $\pi_1(2n) = \pi(2n) - \pi_3(2n)$, where for convenience, $\pi(2n)$ denotes the number of odd primes $\leq 2n$.

Clearly

$$1 < R/\prod_{s=1}^{n} (s^2) = \binom{2n}{n} \cdot R/(2n)!\,.$$

$\binom{2n}{n} < 2^{2n}$, and $(2n)! = 2^{a_{2n}(2)} \cdot \prod_{p \leq 2n} p^{a_{2n}(p)} \cdot \prod_{q \leq 2n} q^{a_{2n}(q)}$.

It is easily seen that $a_{2n}(2) > 2n - 2 - \log(2n)/\log 2$, and thus

https://doi.org/10.1017/S0008439500026801 Published online by Cambridge University Press

$2^{a_{2n}(2)} > 2^{2n}/(8n)$. It follows from this and (2), that

$$1 < \left\{ 2^{2n} \, 2^{(n+1)/2} \, (2n)^{2.\pi(2n)} \right\} \Big/ \left\{ (2^{2n}/8n) \, . \prod_{q \leq 2n} q^{a_{2n}(q)} \, . \, (2n)^{2\pi_3(2n)} \right\}$$

or

$$(3) \qquad \prod_{q \leq 2n} \left\{ q^{a_{2n}(q)} \, . \, (2n)^2 \right\} < n \, . \, 2^{(n+7)/2} \, . \, (2n)^{2\pi(2n)} \, .$$

Now

$$\log \left\{ q^{a_{2n}(q)} . (2n)^2 \right\} > \left\{ a_{2n}(q) + \log(2n)/\log q \right\} . \log q > 2n . \sum_r \log q/q^r$$

$$(q^r \leq 2n) \, .$$

It follows from (3) that

$$2n . \sum_{q^r \leq 2n} \log q/q^r < 2 . \pi(2n) . \log(2n) + (n+7)(\log 2)/2 + \log n .$$

But $\pi(2n) \, . \, \log(2n) < 1.26 \cdot (2n)$;

[see, e.g., J. B. Rosser and L. Schoenfeld, Approximate Formulas for some Functions of Prime Numbers, Illinois J. vol. 6, pp. 64-93].

Thus

$$(4) \qquad \sum_{q^r \leq 2n} \log q/q^r < 2.52 + (\log 2)/4 + (\log n + 2.45)/(2n)$$

$$< 2.8 \quad \text{for} \quad 2n \geq 1000 .$$

But it is just a matter of patience to show that $\sum_{q^r \leq 1000} \log q/q^r > 2.9$.

Thus R cannot be a square for $n \geq 500$. Therefore $n < 500$. $36^2 + 1 = 1297$ is a prime greater than $2n$; thus $n < 36$.

https://doi.org/10.1017/S0008439500026801 Published online by Cambridge University Press

Again, $10^2 + 1 = 101$ is a prime $> 2n$; by (1), R cannot contain this factor, thus $n < 10$.

Finally, $4^2 + 1 = 17$ is not contained in $s^2 + 1$ for $4 < s < 10$, and thus $n \leq 3$. But for $n = 3$, $R = 2 \cdot 5 \cdot 10$ <u>is</u> a square, and

$$\tan^{-1} 1 + \tan^{-1} 2 + \tan^{-1} 3 = 2(\pi/2) .$$

<u>P 66</u>. "Gauss' Lemma" (§ 23, vol. 1 of Modern Algebra by Van der Waerden) is essentially equivalent to the statement that a unique factorization domain R has the following property:

(*) If K is the field of quotients of R, then a polynomial over R which factors over K factors over R.

Show that the following converse holds: if R is a domain in which every element can be expressed as a product of irreducible elements - for example if R is Noetherian - and if R has property (*), then R is a unique factorization domain.

Carl Riehm, McGill University

<u>Solution by L. Carlitz, Duke University.</u>

Assume that R is not a unique factorization domain but that every element of R can be expressed as a product of prime elements. Then there exist elements $a, b, c, p \in R$ such that $pa = bc$, p prime and $p \nmid b$, $p \nmid c$. Consider the product

$$(px+b)(px+c) = p^2x^2 + p(b+c)x + bc ,$$

where x is an indeterminate. Thus we have the following factorization in K[x]:

$$f(x) = px^2 + (b+c)x + a = (px+b)(x+\frac{c}{p}) .$$

Now assume that f(x) admits of a factorization in R[x]; then we must have

$$px^2 + (b+c)x + a = (px+r)(x+s) \quad (r, s \in R).$$

Equating coefficients we get

$$r + ps = b+c, \quad r(ps) = bc.$$

It follows that either $r = b$, $ps = c$ or $r = c$, $ps = b$. Since either alternative violates $p \nmid b$, $p \nmid c$ we have a contradiction.

Also solved by J. D. Dixon, and the proposer.

Editor's comment: Property (*) restricted to monic polynomials is equivalent to R being integrally closed in K (for any domain R).

P 67. Let

$$C = \lim_{n\to\infty} \left[\sum_{j=1}^{n} \frac{1}{j} - \ell n\, n \right]$$

(the Euler-Mascheroni constant) and let x be a real variable. Determine the following limit:

$$\lim_{x\to 0} x^{-2} \{ C + \mathcal{R}(\Gamma'(ix)/\Gamma(ix)) \},$$

where $\mathcal{R}$ = real part of.

H. G. Helfenstein, University of Ottawa

Solution by A. E. Livingston, University of Alberta.

We have

$$\frac{\Gamma'(z)}{\Gamma(z)} = - C - \frac{1}{z} + \sum_{n=1}^{\infty} \left(\frac{1}{n} - \frac{1}{z+n} \right)$$

for $z \neq 0, -1, -2, \ldots$ [E. T. Whittaker and G. N. Watson, A Course of Modern Analysis, 4th ed., Cambridge (1952), p. 247].

https://doi.org/10.1017/S0008439500026801 Published online by Cambridge University Press

Thus,

$$x^{-2}\{C+\mathcal{R}(\Gamma'(ix)/\Gamma(ix))\} = \sum_{n=1}^{\infty} \frac{1}{n|ix+n|^2} \to \sum_{n=1}^{\infty} \frac{1}{n^3}$$

as $x \to 0$.

(A perhaps more elegant but somewhat longer solution to this problem can be obtained by observing that the desired limit is

$$\lim_{x\to 0} x^{-2}\mathcal{R}\left[\int_0^1 (1-t^{ix})/(1-t)\,dt\right].$$

Now write $[0,1]$ as $[0,e^{-\pi}]\cup[e^{-\pi},1]$ and apply Lebesgue's Principle of Dominated Convergence on $[0,e^{-\pi}]$, and the Principle of Monotonic Convergence on $[e^{-\pi},1]$. The result is $2^{-1}\int_0^1 \ell n^2\, t/(1-t)\,dt$, which is easily seen to have the value $\Sigma_1^\infty 1/n^3$.)

Editor's comment: From $\Gamma(z+1) = z\Gamma(z)$ one obtains

$$\frac{\Gamma'(z+1)}{\Gamma(z+1)} = \frac{1}{z} + \frac{\Gamma'(z)}{\Gamma(z)}$$

and therefore

$$\mathcal{R}\left(\frac{\Gamma'(ix+1)}{\Gamma(ix+1)}\right) = \mathcal{R}\left(\frac{\Gamma'(ix)}{\Gamma(ix)}\right)$$

when x is real. From Whittaker and Watson we have,

$$C + \frac{\Gamma'(ix+1)}{\Gamma(ix+1)} = \int_0^1 (1-t^{ix})/(1-t)dt .$$

This observation is necessary since the principle of dominated convergence cannot be applied (near $t=0$) to the corresponding integral for $C + \Gamma'(ix)/\Gamma(ix)$.

Also solved by J. S. Muldowney and the proposer.

P 68. Find all solutions of

$$\varphi(2^{2^n} - 1) = \varphi(2^{2^n}),$$

where φ is Euler's function.

David Klarner, University of Alberta

Solution by H. L. Abbott, University of Alberta.

Since φ is a multiplicative function and $2^{2^i} + 1$ and $2^{2^j} + 1$ are relatively prime if $i \neq j$, our problem is reduced to solving for n the following equation:

$$(1) \qquad \prod_{i=0}^{n-1} \varphi(2^{2^i} + 1) = 2^{2^n - 1}.$$

It is well known that $2^{2^5} + 1$ is divisible by 641, so that $\varphi(2^{2^5} + 1)$ is not a power of 2. Hence (1) has no solutions for $n \geq 6$. For $0 \leq i \leq 4$, $2^{2^i} + 1$ is a prime, and hence for $1 \leq n \leq 5$ we have

$$\prod_{i=0}^{n-1} \varphi(2^{2^i} + 1) = \prod_{i=0}^{n-1} 2^{2^i} = 2^{2^n - 1}.$$

The only solutions are therefore $n = 0, 1, 2, 3, 4, 5$. (The solution $n=0$ is not covered by the above argument, but is easily seen to be a solution of the original equation.)

Also solved by W. J. Blundon, L. Carlitz, J. D. Dixon, L. Moser and the proposer.

https://doi.org/10.1017/S0008439500026801 Published online by Cambridge University Press

P 69. It is a familiar fact that a cyclic permutation of length n can be written as a product of n-1 transpositions. Show that it cannot be done so more economically.

I. Connell, McGill University

Solution by John Dixon, California Institute of Technology.

Since an n-cycle generates a transitive permutation group, the result to be proved is implied by the stronger assertion: n-2 transpositions cannot generate a transitive permutation group of degree n. The latter statement is proved as follows.

Suppose the transpositions $(a_i\, b_i)$ $(i = 1, 2, \ldots, s)$ generate a transitive permutation group G on the symbols $1, 2, \ldots, n$. We define an associated graph whose vertices are labelled 1 to n and whose edges are (a_i, b_i) $(i = 1, 2, \ldots, s)$. The fact that G is transitive implies that the graph is connected.

We now prove by induction on n that a connected graph with n vertices must have $\geq n-1$ edges $(n \geq 2)$. Each vertex must have at least one incident edge. If every vertex has at least two incident edges, then the graph clearly has $\geq n$ edges. On the other hand, if one vertex has only one edge, then after removing this vertex and the corresponding edge, we have a graph with n-1 vertices which is also connected. By the induction hypothesis, this latter graph has $\geq n-2$ edges. Therefore, the original graph has $\geq n-1$ edges.

Also solved by L. Carlitz, H. Gonshor and C. Riehm; they generalized the problem in other directions.

P 70. Prove that every finite abelian group is isomorphic to a subgroup of the multiplicative group of integers relatively prime to m, mod m, for suitable m.

Carl Riehm, McGill University

Solution by H. Gonshor, Rutgers University.

According to a well known theorem in number theory,

https://doi.org/10.1017/S0008439500026801 Published online by Cambridge University Press

prime numbers have primitive roots. In algebraic language this says that the multiplicative group of integers prime to P is cyclic. The order is $P-1$.

Furthermore if M and n are relatively prime then the multiplicative group of integers prime to Mn is the direct sum of the multiplicative group of integers prime to M and the multiplicative group of integers prime to n. Hence the multiplicative group of integers prime to $P_1, P_2, \ldots, P_n$ is the direct sum of the cyclic groups of order $P_1-1, P_2-1, \ldots, P_n-1$.

Every finite abelian group is a direct sum of cyclic groups. Let the cyclic groups involved have orders $r_1, r_2, \ldots, r_n$. We now choose primes $P_1, P_2, \ldots, P_n$ all distinct so that $r_i | P_i-1$. This can always be done since for fixed r the arithmetic progression $1+nr$ contains infinitely many primes by Dirichlet's theorem. By elementary group theory the cyclic group of order r_i is a subgroup of the cyclic group of order P_i-1; hence the direct sum of cyclic groups of orders r_i is a subgroup of the direct sum of cyclic groups of order P_i-1. Thus the given abelian group is a subgroup of the multiplicative group of integers prime to $P_1, P_2, \ldots, P_n$. This proves a stronger form of the statement of the problem, - namely that m may be chosen so that it has no repeated prime factors.

Also solved by J. O. Brooks, L. Carlitz and the proposer.

Editor's comment: The result appears as a theorem in Shanks, Number Theory, vol. 1 (Spartan, 1962), p. 96. There is a standard elementary proof, using cyclotomic polynomials, of the special case of Dirichlet's theorem that $1+nr_i$ $(n=1, 2, \ldots)$ contains infinitely many primes. However the r_i above may actually be taken to be prime powers, and for this case Shanks gives a completely elementary proof, using only Fermat's theorem.