SUPER SIX PROBLEMS ON PRIMES*

Prof. K. Raja Rama Gandhi  Number Theorist, BITS-Vizag, Andhra Pradesh, INDIA

Email: rrmath28@gmail.com

ABSTRACT

In this paper, we discuss some investigations on primes by proofs. We can see many problems and observations during the classroom teaching. With my utmost interest, whatever observations/note took place in my regular reading/teaching, few of them answered by proofs with good analysis.

Keywords: primes, quadratic residue, Wilson’s Theorem

MSC: 11A15, 11T30, 11A51

1 Introduction

Euclid, an ancient Greek philosopher, proved that the number of prime numbers is infinite. Another ancient Greek, Eratosthenes, described a mathematical “sieve” to filter out composite numbers that are the products of the first primes found. These two Greeks allow us to say, without being too rigorous, that the number of prime numbers must be a “countable” infinity. Future articles in this series may include specific types of prime numbers, and ways in which prime numbers are used. Leonhard Euler is a modern mathematician who contributed to the study of prime numbers. One use for prime numbers familiar to many in the fields of cryptography and of computer security is to multiply a pair of large prime numbers for data encryption. Because it is difficult to determine factors of a large number, this is a fairly secure way of encrypting computer data. Whether faster algorithms or “quantum computing” will ever make this approach obsolete are questions that remain unsolved. In this paper, few of my observations on primes with proofs are given.

2 FIRST TWO OF THEM

(1) Prove that the equation \(1 + x + x^2 = py\) has integer solutions for infinitely many primes \(p\).

(2) Twin primes are those differ by 2. Show that 5 is the only prime belonging to two such pairs. Show also that there is a one-to-one correspondence between twin primes and positive integers \(n\) such that \(d(n^2 - 1) = 4\) whereas above \(d(k)\) stands for the number of divisors of \(k\).

Proof of (1): The proof is a modification of the "Euclid" proof [1] that there are infinitely many primes. Let \(p_1 = 3\) and by Putting \(x = 1\) and \(y = 1\), we see that \(1 + x + x^2 = py\) has a solution. Now suppose that we have found \(n\)
primes \( p_1, p_2, \ldots, p_n \) such that \( 1 + x + x^2 = py \) has a solution for any \( i \) from 1 to \( n \). We exhibit a new prime \( p_{n+1} \) such that \( 1 + x + x^2 = py \) has a solution. Consider the number 
\[ 1 + (p_1 p_2 \cdots p_n) + (p_1 p_2 \cdots p_n)^2. \]
This is an integer \( > 1 \), so has a prime divisor \( p_{n+1} \). For any such \( p_{n+1} \), must be distinct from \( p_1, p_2, \ldots, p_n \). This is because if \( p_{n+1} = p_i \), where \( 1 \leq i \leq n \), then \( p_i \) divides \( (p_1 p_2 \cdots p_n) + (p_1 p_2 \cdots p_n)^2 \) \( \Rightarrow \) cannot divide \( 1 + (p_1 p_2 \cdots p_n) + (p_1 p_2 \cdots p_n)^2 \).

Therefore, we have found a new prime \( p_{n+1} \) such that \( 1 + x + x^2 = p_{n+1} y \) has a solution.

**Proof of (2):** The number 5 belongs to the pairs (3, 5) and (5, 7). It is clear that 2 do not belong to any pair, and 3 belong to only 1 pair. We show that any prime \( p \geq 7 \) cannot belong to more than one pair. Suppose to the contrary that \( p \) does. Then \( p - 2, p, \) and \( p + 2 \) are prime. Note that if \( x \) is any integer, then one of \( x - 2, x, \) or \( x + 2 \) is divisible by 3. A number divisible by 3 and greater than 3 never be a prime.

For the second part of the question, we ask when \( d(n^2 - 1) = 4 \). If \( n \) is even, then \( n - 1 \) and \( n + 1 \) are relatively prime, so 
\[ d((n-1)(n+1)) = d(n-1)d(n+1). \]
But 1 is the only \( k \) such that \( d(k) = 1 \). So we must have 
\[ d(n-1) = d(n+1) = 2. \]
That forces the pair \( (n-1, n+1) \) to be a pair of twin primes.

Now examine the cases \( n \) odd. Then \( (n-1)(n+1) \) is divisible by 8, so has the divisors 1, 2, 4 and 8. Since \( d(n^2 - 1) = 4 \), it can have no others. Thus \( (n^2 - 1) = 8 \), giving \( n = 3 \). So the set \( A \) of numbers \( n - 1 \) such that \( d(n^2 - 1) = 4 \) consist of 2 plus the smaller primes in a twin prime pair [2]. This set can be easily put in one to one correspondence with the set \( B \) of smaller primes in twin prime pairs. Just list the two sets as \( a_1, a_2, \ldots \) and \( b_1, b_2, \ldots \) and map \( a_i \) to \( b_i \). But the one-to-one correspondence bit has absolutely **nothing** to do with twin primes. For **any** two infinite sets of natural numbers can be put in one to one correspondence.

### 3 Next Two of Them

(3) Can we represent any prime \( p \equiv 1 \pmod{3} \) in terms of \( (a + b)^2 - ab \) with \( a > b > 0 \)?

(4) Can we represent any prime \( p \equiv \pm 1 \pmod{5} \) in terms of \( (a + b)^2 + ab \) with \( a > b > 0 \)?

**Proof of (3):** If \( p \equiv 1 \pmod{3} \), then -3 is the quadratic residue [4] modulo \( p \). That means, there exist some integer \( x \) such that \( p | (x^2 + 3) \). Now we move to \( O_{-3} \), the ring of integers [3] in the number field \( K = \mathbb{Q}(\sqrt{-3}) \), and we write 
\[ p | (x - \sqrt{-3})(x + \sqrt{-3}) \]. Clearly \( p \) does not divide either one of \( (x \pm \sqrt{-3}) \), since \( \left( \frac{x \pm \sqrt{-3}}{p} \right) \) are not in \( O_{-3} \). But it is known that \( O_{-3} \) is a unique factorization domain, implying that if an irreducible divides a product it must divide one of the factors. We deduce that \( p \) is not an irreducible in \( O_{-3} \). Let
\[ \pi = a + b \frac{1 + \sqrt{3}}{2} \] be a nontrivial factor of \( p \) in \( \mathcal{O}_3 \).

Then the norm of \( \pi \) is a positive nontrivial factor of the norm of \( p \), which is \( p^2 \), so the norm of \( \pi \) is \( p \).

But the norm of \( \pi \) is \( (a + b)^2 - ab \).

**Proof of (4):** If \( p \equiv \pm 1(\text{mod} 5) \), then 5 is a quadratic residue modulo \( p \), then \( p \mid (x^2 - 5) \) for some \( x \). Now for \( \mathcal{O}_5 \), \( p \mid (x - \sqrt{5})(x + \sqrt{5}) \). As like our previous solution, \( p \) divides either one of \( x \pm \sqrt{5} \). Since \( \mathcal{O}_5 \) is known to be UFD [6], so, \( p \) is again not irreducible in \( \mathcal{O}_5 \). Let

\[ \pi = a + b \frac{1 + \sqrt{5}}{2} \] be a non-trivial factor of \( p \) in \( \mathcal{O}_5 \). Now by taking norms, we can see that \( p = a^2 + ab - b^2 \). By simple substitution, we get \( (a + b)^2 + ab \).

**4 LAST TWO OF THEM**

**5** If \( (6n - 1, 6n + 1) \) are said to be twin primes except \( (3, 5) \), then the following congruence is true: \( 4(6n - 2)! \equiv -3(1 + 2n)(\text{mod} 36n^2 - 1) \).

**6** For a positive odd integer \( p \) and for any two distinct odd primes \( p_1 \) and \( p_2 \) with

\[ p_1 + p_2 - p = 1, \]

then \( (p - p_1)(p - p_2) ! \equiv -1(\text{mod} p) \) \( \iff \) \( p \) is prime.

**Proof of (5):** As we know that, Wilson’s Theorem [5] \( (p - 1)! \equiv -1(\text{mod} p) \) \( \iff \) \( p \) is prime. If we assume \( 6n - 1 \) and \( 6n - 2 \) are primes \( \Rightarrow (6n - 2)! \equiv -1(\text{mod}(6n - 1)), \) and

\( (6n)! \equiv -1(\text{mod}(6n + 1)). \)

Similarly, the second congruence can be expressed as

\( (6n - 2)! \equiv -1(-1)^{-1}(-2)^{-1} = -2^{-1}(\text{mod}(6n + 1)). \)

Now, by multiplying both the congruencies by 4

\( 4(6n - 2)! \equiv -4(\text{mod}(6n - 1)) \)

yields:

\( 4(6n - 2)! \equiv -2(\text{mod}(6n + 1)) \)

Now, by checking we realize that, these are indeed the residues of \(-3(1 + 2n)\).

**Note:** If we write twin prime pairs \( (p, p + 2) \) in (5), we see \( 4(p - 1)! \equiv -4 - p(\text{mod}(p^2 + 2p)) \).

**Proof of (6):** As we know that,

\( n! \equiv (-1)^n(p - 1)(p - 2)...(p - n) \equiv \frac{(-1)^n(p - 1)!}{(p - n)!}(\text{mod} p) \)

\( \Rightarrow n!(p - n - 1)! \equiv (p - 1)! \equiv -1(\text{mod} p) \).

For \( n \) is even and by Wilson’s Theorem [5] \( p \) is obviously prime. Consider \( n = p - p_1 \) (even) and note that \( p_1 - 1 = p - p_2 \) to get one way. In another way, note that, if \( p \) is not prime, then it is divisible by some prime \( q \leq (p - 1)/2 \). Of course, we cannot hold both \( q > p - p_1 \) and \( q > p - p_2 \) (since \( p_1 + p_2 - p = 1 \) would contradict \( q \leq (p - 1)/2 \) \( \Rightarrow \) \( q \) must divide at least one of \( (p-p_1) \) ! And \( (p-p_2)! \), when their product different from \(-1 \text{ (mod} p) \).

**Acknowledgements**

I am heartily thankful to Mathematician Prof. J. Gopala Krishna and my well-wishers Smt. Sri Lakshmi (secretary and correspondent of BITS-Vizag), Dr. C.V. Gopinath, G. merson and Prof. A. Nicolas, whose encouragement, guidance and support from the initial to the final level enabled me to develop an understanding of the subject.
REFERENCES

USA, 2011

Springer+Business Media LLC 2011.

New York, Inc. 2004


Academic Press, USA, 1999

2002