MISCELLANEOUS RESULTS ON PRIME NUMBERS

A. M. KASPRZYK

Many of the following results, along with much more, can be found in *An Introduction to the Theory of Numbers* by G. H. Hardy and E. M. Wright (Oxford Science Publications, OUP, 1979).

Definition 0.1. A number $p \in \mathbb{Z}$ is called a *prime number* if $p \geq 2$ and p has no factors except ± 1 and $\pm p$

Theorem 0.2. *Let p be a prime number and let $b, c \in \mathbb{Z}$. Suppose that $p \mid bc$, then $p \mid b$ or $p \mid c$.*

Proof. Suppose $p \nmid b$. Then $(p, b) = 1$ since the only factors of p and ± 1 and $\pm p$. Thus there exist $\lambda, \mu \in \mathbb{Z}$ such that $1 = \lambda p + \mu b$. Hence $c = \lambda cp + \mu cb$. But p divides the r.h.s., and hence p must divide c. $\square$

Theorem 0.3 (The Infinitude of Primes)**.** *There are infinitely many primes.*

Proof. Suppose that the number of primes is finite, with the set of all prime numbers being equal to $\{2, 3, 5, \ldots, p_r\}$. Let

$$q = 2 \cdot 3 \cdot 5 \cdot \ldots \cdot p_r + 1$$

where p_r is the r^{th} prime number. Let p be a prime dividing q. Then p cannot be any of $p_1, p_2, \ldots, p_r$ since $q \equiv 1$ $(mod\ p_i)$ $(i = 1, 2, \ldots, r)$. Thus this prime p is a prime not in our original list, and so we obtain the desired contradiction. $\square$

Theorem 0.4 (Fermat's Little Theorem)**.** *Let p be a prime and let $a \in \mathbb{Z}$ be such that $p \nmid a$. Then $a^{p-1} \equiv 1$ $(mod\ p)$.*

Proof. Start by listing the first $p - 1$ positive multiples of a

$$a, 2a, 3a, \ldots, (p-1)a$$

Suppose that ra and sa are the same modulo p. Then we have $r \equiv s$ $(mod\ p)$, which is not possible. Thus the $p - 1$ multiples of a above are distinct and non-zero. Thus they must be congruent to $1, 2, 3, \ldots, p-1$ (in some order). Multiply all these congruences together and we find

$$a \cdot 2a \cdot 3a \cdot \ldots \cdot (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1) \quad (mod\ p)$$

and hence

$$a^{p-1}(p-1)! \equiv (p-1)! \pmod{p}.$$

Dividing both sides by $(p-1)!$ gives the result. □

Corollary 0.5. *Let p be a prime and $a \in \mathbb{Z}$. Then $a^p \equiv a \ (mod\ p)$.*

Proof. The result is trivial if $p \mid a$ (since both sides are 0). If $p \nmid a$ then simply multiply the congruence in Fermat's Little Theorem by a to get the desired result. □

Theorem 0.6 (Wilson's Theorem)**.** *Let p be an integer greater than 1. We have that p is prime if and only if $(p-1)! \equiv -1 \ (mod\ p)$.*

Proof. The result is clearly true if $p = 2$ or 3, so let us assume $p > 3$. If p is composite, then its positive divisors are among the integers

$$1, 2, 3, \ldots, p-1$$

and it is clear that $g.c.d.\{(p-1)!, p\} > 1$, so we cannot have $(p-1)! \equiv -1 \ (mod\ p)$.
If p is prime then each of the above integers are relatively prime to p. So for each of these integers a there exists $\lambda, \mu \in \mathbb{Z}$ such that $\lambda a + \mu p = 1$. Hence $\lambda a \equiv 1 \ (mod\ p)$. It is important to note that this λ is unique modulo p, and that since p is prime, $a = \lambda$ if and only if a is 1 or $p-1$. Now if we omit 1 and $p-1$ then the others can be grouped into pairs whose product is

$$2 \cdot 3 \cdot \ldots \cdot (p-2) \equiv 1 \pmod{p}.$$

Finally we simply multiply both sides by $p-1$ to obtain our result. □

Theorem 0.7. *Let p be prime. Then $\sqrt{p}$ is irrational.*

Proof. Let $p \in \mathbb{N}$ be prime, and for a contradiction suppose that

$$\sqrt{p} = \frac{q}{r} \in \mathbb{Q}$$

where $q, r \in \mathbb{N}$ are coprime, $r \neq 1$. Then we have that

$$pr^2 = q^2 \tag{0.1}$$

and hence that $p \mid q^2$.

Suppose that $p \nmid q$. By the uniqueness of prime factorization we have that there exist (not necessarily distinct) primes $p_i \neq p$ such that

$$q = p_1 \ldots p_n.$$

Thus $q^2 = p_1^2 \ldots p_n^2$ and so $p \nmid q^2$, which is a contradiction. Hence we must have that $p \mid q$.

We may thus write $q = pk$ for some $k \in \mathbb{N}$, and equation (0.1) gives us that

$$pr^2 = p^2 k^2.$$

Dividing through by p we have that $r^2 = pk^2$ and thus that $p \mid r^2$. By the same argument as above this gives us that $p \mid r$.

So we have shown that $p \mid r$ and $p \mid q$, and so q and r are not coprime, which contradicts our original hypothesis. Hence it must be that $\sqrt{p}$ is irrational. □

Theorem 0.8. $3, 5, 7$ *are the only three consecutive odd numbers which are prime.*

Proof. One of $n, n+2, n+4$ must be divisible by 3. □

Theorem 0.9. *If for some* $n \in \mathbb{N}, 2^n - 1$ *is prime, then so is* n.

Proof. Let $r, s \in \mathbb{N}$. Then we have

$$x^{rs} - 1 = (x^s - 1)(x^{s(r-1)} + x^{s(r-2)} + \ldots + x^s + 1).$$

So if n is composite (say $n = rs$ with $1 < s < n$) then $2^n - 1$ is also composite (because it is divisible by $2^s - 1$). □

Corollary 0.10. *Let* a *and* n *be integers greater than* 1. *If* $a^n - 1$ *is prime then* $a = 2$ *and* n *is prime.*

Proof. Since $x - 1$ divides $x^n - 1$, for the latter to be prime the former must be equal to 1. □

Theorem 0.11. 3 *is the only prime number of the form* $2^{2n} - 1$.

Proof. $2^{2n} - 1 = (2^n - 1)(2^n + 1)$, so for the l.h.s. to be prime we require $2^n - 1 = 1$. □

Theorem 0.12. *There are infinitely many primes of the form* $4n + 3$.

Proof. Define

$$q = 2^2 \cdot 3 \cdot 5 \cdot \ldots \cdot p_r - 1$$

where p_r is the r^{th} prime number (c.f. proof of the Infinitude of Primes).
Then q is of the form $4n + 3$ and is not divisible by any of the primes up to p_r. It cannot be a product of primes only of the form $4n + 1$ since the product of two numbers of this form is also of this form. Thus it is divisible by a prime of the form $4n + 3$ greater than p_r. □

Theorem 0.13. *There are infinitely many primes of the form* $6n + 5$.

Proof. This proof is very similar to the previous one.
Define

$$q = 2 \cdot 3 \cdot 5 \cdot \ldots \cdot p_r - 1$$

and observe that any prime number except 2 or 3 is of the form $6n + 1$ or $6n + 5$, and that the product of two numbers of the form $6n + 1$ is of the same form. □