- 16. Let a and b be nonzero integers. If there exists r and s such that ar +bs = 1. Show that a and b are relatively prime.

- 19. Let $x, y \in N$ be relatively prime. If xy is a perfect square, prove that x and y must both be perfect squares.

- 28. Let $p>=2$. Prove that if $2^p -1$ is prime then p is also prime.

Mersenne primes.

- **If p is a prime, 2^p -1 is not necessarily a prime. E.g., 2^11 – 1 = 2047 = 23*89.**

- **Definition:** When $2n$-1 is prime it is said to be a **Mersenne prime**.

$P^2 = 2q^2$

- Using the fact that 2 is a prime, show that there do not exist integers p and q such that $p^2 = 2q^2$.

There are various proofs of this result. Since you are asked to use the fact that 2 is prime, possibly the following one is intended.

Suppose that $p^2 = 2q^2$, and factorise each side into primes. Since p^2 is a square, the number of factors of 2 on the LHS is even. Similarly, the number of factors of 2 in q^2 is even; but the extra 2 makes the number of factors of 2 on the RHS odd. Therefore LHS cannot equal RHS.

Infinite 4k-1 primes

- 30. Prove that there are an infinite number of primes of the form 4k-1.

- 假设4k-1形素数只有n个，分别为p1,p2,……,pn
考虑N=4p1p2……pn-1,设N的标准分解为
N=q1q2……qm，即有4p1p2……pn-1=q1q2……qn
因为qi(i=1,2,……，m)为质数，所以只有4k+1和4k-1形
若某个qi为4k-1形，则有
qi=pj(i=1,2,……,m;j=1,2,……，n),则有qi丨-1，矛盾
若qi都是4k+1形，两边对4求余有-1=1(mod4),又矛盾
所以形如4k+3形素数有无穷多个

Infinite 6n+1 primes

- Prove that there are an infinite number of primes of the form $6n + 1$.

Dirichlet’s Theorem

- In number theory, **Dirichlet's theorem**, also called the Dirichlet prime number theorem, states that for any two positive coprime integers *a* and *d*, there are infinitely many primes of the form $a + nd$, where n is a non-negative integer.
- This result had been conjectured by Gauss, but was first proved by Dirichlet (1837).

8. If $k = jq + r$, as in Euclid's division theorem, is there a relationship between $\gcd(q, k)$ and $\gcd(r, q)$? If so, what is it?

15. If $k = jq + r$, as in Euclid's division theorem, is there a relationship between $\gcd(j, k)$ and $\gcd(r, k)$? If so, what is it?

The end.

Infinite primes

- Euclid offered the following proof published in his work *Elements* (Book IX, Proposition 20),[1] which is paraphrased here.
- Consider any finite list of prime numbers $p1$, $p2$, ..., pn. It will be shown that at least one additional prime number not in this list exists. Let P be the product of all the prime numbers in the list: $P = p1p2...pn$. Let $q = P + 1$. Then q is either prime or not:
- If q is prime, then there is at least one more prime than is in the list.
- If q is not prime, then some prime factor p divides q. If this factor $p$were on our list, then it would divide P (since P is the product of every number on the list); but p divides $P + 1 = q$. If p divides $P$and q, then p would have to divide the difference[2] of the two numbers, which is $(P + 1) - P$ or just 1. Since no prime number divides 1, this would be a contradiction and so p cannot be on the list. This means that at least one more prime number exists beyond those in the list.
- This proves that for every finite list of prime numbers there is a prime number not on the list, and therefore there must be infinitely many prime numbers.
- Euclid is often erroneously reported to have proved this result bycontradiction, beginning with the assumption that the set initially considered contains all prime numbers, or that it contains precisely the $n$smallest primes, rather than any arbitrary finite set of primes.[3] Although the proof as a whole is not by contradiction (it does not assume that only finitely many primes exist), a proof by contradiction is within it, which is that none of the initially considered primes can divide the number $q$above.