

the order of magnitude of $\pi(x)$. The limit is of course an absurdly weak one, since for $x = 10^9$ it gives $\pi(x) \geq 3$, and the actual value of $\pi(x)$ is over 50 million.

2.3. Primes in certain arithmetical progressions. Euclid's argument may be developed in other directions.

THEOREM 11. *There are infinitely many primes of the form $4n+3$.*

Define q by
$$q = 2^2 \cdot 3 \cdot 5 \cdots p - 1,$$
 instead of by (2.1.1). Then q is of the form $4n+3$, and is not divisible by any of the primes up to p . It cannot be a product of primes $4n+1$ only, since the product of two numbers of this form is of the same form; and therefore it is divisible by a prime $4n+3$, greater than p .

THEOREM 12. *There are infinitely many primes of the form $6n+5$.*

The proof is similar. We define q by

$$q = 2 \cdot 3 \cdot 5 \cdots p - 1,$$

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

The progression $4n+1$ is more difficult. We must assume the truth of a theorem which we shall prove later (§ 20.3).

THEOREM 13. *If a and b have no common factor, then any odd prime divisor of a^2+b^2 is of the form $4n+1$.*

If we take this for granted, we can prove that there are infinitely many primes $4n+1$. In fact we can prove

THEOREM 14. *There are infinitely many primes of the form $8n+5$.*

We take
$$q = 3^2 \cdot 5^2 \cdot 7^2 \cdots p^2 + 2^2,$$

a sum of two squares which have no common factor. The square of an odd number $2m+1$ is

$$4m(m+1)+1$$

and is $8n+1$, so that q is $8n+5$. Observing that, by Theorem 13, any prime factor of q is $4n+1$, and so $8n+1$ or $8n+5$, and that the product of two numbers $8n+1$ is of the same form, we can complete the proof as before.

All these theorems are particular cases of a famous theorem of Dirichlet.

THEOREM 15* (DIRICHLET'S THEOREM).[†] *If a is positive and a and b have no common divisor except 1, then there are infinitely many primes of the form $an+b$.*

[†] An asterisk attached to the number of a theorem indicates that it is not proved anywhere in the book.