The basic results on sums of squares depend on the theory of quadratic residues, so this chapter is a natural continuation of the previous one.

So it looks like every number is the sum of four squares and it seems that the primes  $p \equiv 1 \pmod{4}$  always have a representation, but those  $\equiv 3 \pmod{4}$  never have one. But what about general n? Fermat found a rule

which tells us precisely which numbers are the sum of two squares. Eventually Lagrange proved the four square theorem.