Section 2.5
Carl Friedrich Gauss

Who: Perhaps the greatest mathematician of all time

What: Number theory moves into its modern period

When: 1777-1855

It is unfair to a few great mathematicians to proclaim Gauss as the next great number theorist. However, in the Introduction of our notes I said (in reference to Gauss),

> But not until the end of the 18th century would a mathematician be worthy of being called the successor of Fermat.

We will begin this section by briefly discussing those being dissed, and then move on the great Carl Friedrich Gauss.

From Fermat to Gauss

A quick glance through our Famous Number Theorists Chronology (between Fermat and Gauss) yields quite an impressive list of names that would be ignored if we progressed straight from Fermat to Gauss. Isaac Newton, Jacques Bernoulli, Christian Goldbach, Edward Waring, Adrien-Marie Legendre, Joseph Fourier, and Sophie Germain are just some of those ignored heretofore, but most notably absent would be the giants Joseph Lagrange and Leonhard Euler.

Leonhard Euler is by far the most prolific mathematical author of all time. He wrote around 500 papers and books throughout his lifetime, and left volumes of work upon his death. It took the St. Petersburg Academy Journal 47 years to exhaust the information therein.

Joseph Lagrange was almost as diverse a contributor to the many branches of mathematics as was Euler. Regarding number theory, he seemed to have had a special affinity. He succeeded Euler at the Berlin Academy when the former left Prussia to return to Russia.

The Great Gauss

Carl Friedrich Gauss has an impressive if not unusual claim to fame. Legend has it that he was the last mathematician to be knowledgeable of every field of mathematics. In the 100 years after he died, mathematics grew at such a rate, and it such diverse directions, that no one since Gauss can make such an unbelievable claim. His direct contributions are monumental, and he made advancements in the fields of algebra, differential geometry, differential equations, non-Euclidean geometry, complex analysis, real analysis, group theory, topology, and of course number theory. (He also contributed to physics, mechanics, astronomy, geodesy, and magnetism) His achievements in number theory are our main focus.

It is impossible to pinpoint the single item for which Gauss is most famous. In geometry, it is the construction of the 17-gon using only a ruler and compass. In algebra, it is the first completely satisfactory proof of the Fundamental Theorem of Algebra. In number theory, it is his proof of quadratic reciprocity.

Quadratic Reciprocity (*The Short Version*)

little goal: Find all numbers a that are squares modulo a given odd prime, p.

To do this, we simply have to square each number from 1 to $p-1$, and reduce our answers modulo p. If on the other hand, we wish to

BIG GOAL: Find all odd primes p for which a given number a is a square.

then it is a very different question. However, thanks to quadratic reciprocity, it is equally easy. First a few facts,

(i) -1 is a square modulo $p \Leftrightarrow p = 4k+1$ for some k.
(ii) 2 is a square modulo $p \Leftrightarrow (a) \quad p = 8k+1$ or $p = 8k+7$ for some k, or
(iii) a prime $q = 4l+1$ is a square modulo $p \Leftrightarrow p$ is a square modulo q.
(iv) a prime $q = 4l+3$ is a square modulo $p \Leftrightarrow p$ is a not a square modulo q.
(v) a product $a \cdot b$ is a square modulo $p \Leftrightarrow$ both factors are squares or both aren't.

Put this all together and we can achieve our BIG GOAL.

Example: Find all odd primes p such that 35 is a square modulo p.

$35 = 5 \cdot 7$, so it will be a square modulo p depending on whether 5 and 7 are. But 5 (which is 4(1)+1) is a square modulo p if and only if p is a square modulo 5. The only such numbers are 1 and 4. On the other hand, 7 (which is 4(1)+3) is a square modulo p if and only if p is *not* a square modulo 7. The squares modulo 7 are 1, 2, and 4. So p would need to be 3, 5, or 6 modulo 7. Putting these conditions together gives us:

35 is a square modulo p if and only if p is 1 or 4 modulo 5, and
3, 5, or 6 modulo 7.

Hence, 35 is a square modulo the primes 19, 31, 41, 59, 61, etc...

Example: Is 90 a square modulo 331?

$$\left(\frac{90}{331}\right) = \left(\frac{2}{331}\right)\left(\frac{5}{331}\right)\left(\frac{3^2}{331}\right) = (-1)\left(\frac{5}{331}\right)(+1) = (-1)\left(\frac{331}{5}\right)(+1) = (-1)\left(\frac{1}{5}\right)(+1) = (-1)(+1)(+1) = -1$$

So no.