Section 6. Fermat's and Wilson's Theorems

Note. In this section, we prove two theorems concerning congruences modulo a prime. The results are:

Theorem 6.1. Fermat's (Little) Theorem. If p is prime and the greatest common divisor $(a, p) = 1$, then $a^{p-1} \equiv 1 \pmod{p}$.

Theorem 6.2. Wilson's Theorem. Positive integer p is prime if and only if $(p-1)! \equiv -1 \pmod{p}$.

Some of the material in this section is also in my online notes for Mathematical Reasoning (MATH 3000) on Section 6.5. Introduction to Euler's Function.

Note. Pierre de Fermat (August 17, 1601–January 12, 1665) was a French lawyer, government official, and amateur mathematician.

Pierre de Fermat (August 17, 1601–January 12, 1665),

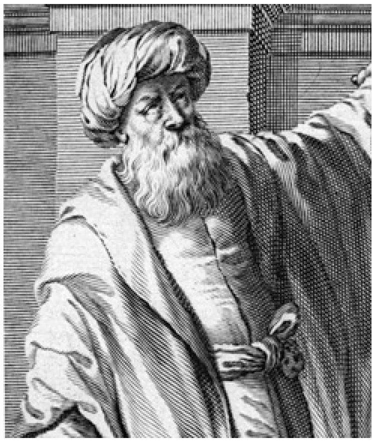
image from Fermat's Library website.

He was friends with several mathematicians of his time and he corresponded with many others. He was recognized as a top mathematician, but he did not bother to give clean, clear proofs of his ideas and he did not publish his work (though some of his ideas made it into publication as supplements to the work of others). He worked in analytic geometry and circulated a manuscript on this topic in 1636 (a year before Descartes published his *La géométrie*). He studied maxima, minima, and tangents to curves (and geometric series) before Newton and Leibniz. He corresponded with Blaise Pascal (June 13, 1623–August 19, 1662) in 1654 about calculating the appropriate payout for a game which was interrupted (and left "unfinished"). This required predicting how the game would end. This correspondence laid the foundations for the idea of probability and Fermat and Pascal are viewed as the founders of probability theory (with Fermat taking the lead role). Here, we are most interested in Fermat's contributions to number theory. While studying perfect numbers (a positive integer is *perfect* if it is equal to the sum of its positive divisors, excluding itself; examples of perfect numbers are 6 and 28—we consider these ideas in Section 8. Perfect Numbers), Fermat discovered his "Little Theorem," which we call in this section simply "Fermat's Theorem" (Theorem 6.1). More famous is "Fermat's Last Theorem." In the margin of a copy of Diophantus' *Arithmetica*, Fermat had written that he had "discovered a truly remarkable proof" that the equation $x^n + y^n = z^n$ has no nonzero solutions x, y, z for $n > 2$; it was common for Fermat to make such claims. In 1670 Fermat's son Samuel published an edition of *Arithmetica* along with his father's notes and this called attention to the problem. The fame of the problem spread as more and more mathematicians failed to find a proof. A proof was finally presented about 300 years later by Andrew Wiles in

1994 (using techniques unavailable to Fermat, so it is agreed that Fermat in fact did not have a "truly remarkable proof"). We give an elementary proof of "Fermat's Last Theorem" (or, as it's called in Dudley, "Fermat's Conjecture"; remember, this book is copyright in 1978) for the case $n = 4$ in Theorem 17.1 of Section 17. Infinite Descent and Fermat's Conjecture. Another problem of Fermat's which we will explore in these notes concerns finding all integer solutions x, y of the equation $x^2 - Ny^2 = 1$; see Section 20. $x^2 - Ny^2 = 1$. This historical information is based on the Wikipedia webpage on Fermat and the MacTutor History of Mathematics Archive page on Fermat.

Note. You may also see a proof of Fermat's (Little) Theorem in Introduction to Modern Algebra (MATH 4127/5127). The proof is based on (1) the fact that the nonzero elements of $\mathbb{Z}_p$, where p is prime, form a group under multiplication, and (2) the fact that the order of a subgroup divides the order of a (finite) group (this is Lagrange's Theorem from group theory). See my online notes for Introduction to Modern Algebra on Section IV.20. Fermat's and Euler's Theorems.

Note. Wilson's Theorem seems to have been first addressed by Ibn al-Haytham (circa 965– circa 1040). English mathematician John Wilson (August 6, 1741–October 18, 1793), who taught at Cambridge, is best known for "Wilson's Theorem," which was first published by Edward Waring (1736–August 15, 1798), though without proof, and was first proved by Joseph-Louis Lagrange (January 25, 1736–April 10, 1813) in 1773. Evidence in his private papers reveal that Gottfried Wilhelm Leibniz (July 1/June 21 1646–November 14, 1716) was also aware of the result.



Ibn al-Haytham

John Wilson

Joseph-Louis Lagrange

Images from Wikipedia (for al Haytham and Lagange) and
MacTutor History of Mathematics Archive (for Wilson), accessed 10/14/2021.

Note. The text book declares Wilson's Theorem "remarkable because it gives a condition both necessary and sufficient for a number to be prime." (See page 43.) Of course (as Dudley also observes), the presence of the factorial makes this computationally impractical because of the large resulting numbers. Notice that both Fermat's and Wilson's Theorems are trivially true for $p = 2$, so in what follows we can assume that prime p is greater than 2. Before proving Fermat's Theorem, we need a lemma.

Lemma 6.1. If the greatest common divisor $(a, m) = 1$, then the least residues of

$$(1)\, a, 2a, 3a, \ldots, (m-1)a \pmod{m} \text{ are (in some order) } (2)\, 1, 2, 3, \ldots, m-1.$$

In other words, if $(a, m) = 1$, then each integer is congruent (mod m) to exactly one of $a, 2a, 3a, \ldots, (m-1)a$.

Note. We are now equipped to prove Fermat's (Little) Theorem (Theorem 6.1).

Note. We can also express the conclusion of Fermat's Theorem as $a^p \equiv a \pmod{p}$. In fact, if $(a, p) \neq 1$ then we must have $(a, p) = p$ since p is prime, and then $a^p \equiv 0 \pmod{p}$ and $a \equiv 0 \pmod{p}$, to that we have the following corollary to Fermat's Theorem.

Corollary 6.A. If p is prime then $a^p \equiv a \pmod{p}$ for all positive a.

Example 6.2. Calculate 2^2 and 2^{10} (mod 11).

Solution. Of course $2^2 \equiv 4 \pmod{11}$. So $2^4 = (2^2)^2 \equiv 4^2 \pmod{11} \equiv 5 \pmod{11}$ and $2^8 = (2^4)^2 \equiv 4^2 \pmod{11} \equiv 5 \pmod{11}$. Then $2^{10} = (2^2)(2^8) \equiv (4)(3) \pmod{11} \equiv 1 \pmod{11}$, as predicted by Fermat's Theorem. □

Note. We now consider a proof of Wilson's Theorem. We need two preliminary lemmas. Notice that the next lemma refers to a number of solutions to the quadratic congruence $x^2 \equiv 1 \pmod{p}$. Recall that by the term "solution" of a linear congruence we mean a least residue modulo p as defined in Section 5. Linear Congruences. We use the term "solution" is the same sense in this quadratic congruence.

Lemma 6.2. The congruence $x^2 \equiv 1 \pmod{p}$, where p is an odd prime, has two solutions: 1 and $p-1$.

Note. The next result concerns the multiplicative inverses modulo prime p. Notice that the result refers to *the* solution of the linear congruence $ax \equiv 1 \pmod{p}$; this linear congruence has a unique solution by Lemma 5.2.

Lemma 6.3. Let p be an odd prime and let a' be the solution of $ax \equiv 1 \pmod{p}$ where $a \in \{1, 2, \dots, p-1\}$. Then $a' \equiv b' \pmod{p}$ if and only if $a \equiv b \pmod{p}$. Furthermore, $a \equiv a' \pmod{p}$ if and only if $a = 1$ or $a = p-1$.

Note 6.A. We know that the multiplicative inverse of $a = 1$ is $a' = 1$, and the multiplicative inverse of $a = p-1$ is $a' = p-1$. Now consider $a, b \in \{2, 3, \dots, p-2\}$ where $a \neq b$. Then $a \not\equiv b \pmod{p}$ and so by Lemma 6.3 we have that the respective inverses a' and b' satisfy $a' \not\equiv b' \pmod{p}$. Now we know that the linear congruence $ax \equiv 1 \pmod{p}$ has a unique solution by Lemma 5.2, so that every $2, 3, \dots, p-2$ has a multiplicative inverse and by Lemma 6.3 the inverse is also one of $2, 3, \dots, p-2$. Since the only elements of $\mathbb{Z}_p$ which are their own inverse are 1 and $p-1$, then the elements of $2, 3, \dots, p-2$ can be paired up into $(p-3)/2$ pairs of the form (a, a').

Note. We are now equipped to prove Wilson's Theorem (Theorem 6.2).

Revised: 4/2/2022