HOMEWORK ASSIGNMENT DUE ON DECEMBER 16

This homework assignment consists of two parts: first, several fairly short problems, most of which are from the book; second, one long problem. In Part 2, consisting of a single, long problem, you will have to bring together several of the things you learned in the course: basic properties of primes, expressing the greatest common divisor of two numbers as an integer linear combination of the numbers, equivalence relations, equivalence classes, functions, bijections.

PART 1

1. Book, page 170, problems 7, 9, 10, 11, 12, 13
2. Book, pages 176, 177, problem 9
3. Book, pages 181 to 183, problems 2, 3, 6, 7, 8, 9, 11. In addition, under the same conditions as in Problem 9, prove or disprove:
   i. if $g \circ f$ is one-to-one then f is one-to-one,
   ii. if $g \circ f$ is one-to-one then g is one-to-one,
   iii. if $g \circ f$ is onto then f is onto,
   iv. if $g \circ f$ is onto then g is onto,
   v. if $g \circ f$ is a bijection then f is a bijection,
   vi. if $g \circ f$ is a bijection then g is a bijection.
4. Prove: if A is a set, then there does not exist a one-to-one function $f : 2^A \mapsto A$. (Hint: let $B = \operatorname{im} f$. Then the function $f^{-1} : B \mapsto 2^A$ is onto. Extend f^{-1} to a function $g : A \mapsto 2^A$. Then use Cantor's theorem.)
5. Construct a bijection $F : \mathbb{R} \mapsto [0, 1]$. (Here $\mathbb{R}$ is the set of all real numbers, and $[0, 1]$ is the closed interval $\{x \in \mathbb{R} : 0 < x < 1\}$.)

PART 2

This part consists of a single problem, in 27—mostly very short—steps. The purpose of this problem is to take you slowly, through the steps of the proof of the following two nontrivial results.

THEOREM 1. *Let p be a prime number. Then the equation $x^2 + y^2 + 1 = 0$ has a solution in $\mathbb{Z}_p$. (That is, there exist members x, y of $\mathbb{Z}_p$ such that $x^2 + y^2 + 1 = 0$ in $\mathbb{Z}_p$.)*

THEOREM 2. *Let p be a prime number such that $p \neq 2$ and $\frac{p-1}{2}$ is odd. Then the equation $x^2 + 1 = 0$ does not have a solution in $\mathbb{Z}_p$. (That is, there does not exist an $x \in \mathbb{Z}_p$ such that $x^2 + 1 = 0$ in $\mathbb{Z}_p$.)*

The things you are asked to do are the 27 steps listed below, labeled S1, S2, up to S27.

Theorem 1 is important because it is the gateway to the proof of a really nice, deeep and rather surprising result, namely, *Lagrange's four-squares theorem*, which says that **every natural number is the sum of four squares**. We are not going to be able to prove this theorem in the course, but Theorem 1 is one of the main ingredients of the proof. (If you are intellectually curious and want to see the complete proof of the Lagrange theorem, you can find it in my Web page.)

Theorem 2 is motivated by the desire to clarify the situation considered in Theorem 1. As we will see, in some cases we can actually do much better than what Theorem 1 says we can do. Indeed, for some primes p we can solve the equation $x^2 + 1 = 0$ in $\mathbb{Z}_p$, in which case of course we also get a solution of $x^2 + y^2 + 1 = 0$ by just taking $y = 0$. This raises the question

QUESTION 1. Is it *always* possible solve the equation $x^2 + 1 = 0$ in $\mathbb{Z}_p$, no matter what the prime p is?

Theorem 2 implies, in particular, that the answer to Question 1 is *no*. In fact, Theorem 2 tells us that there are lots of primes p such that the equation $x^2 + 1 = 0$ cannot be solved in $\mathbb{Z}_p$.

REMARK 1. The following examples may clarify the statements of Theorems 1 and 2:

a. In $\mathbb{Z}_{11}$, we can satisfy $x^2 + y^2 + 1 = 0$ by taking $x = 3$, $y = 1$. This works because in $\mathbb{Z}_{11}$ the equalities $3^2 + 1^2 + 1 = 9 + 1 + 1 = 0$ hold.

b. In $\mathbb{Z}_{13}$, we can satisfy $x^2 + y^2 + 1 = 0$ by taking $x = 5$, $y = 0$. This works because in $\mathbb{Z}_{13}$ the equalities $5^2 + 0^2 + 1 = 25 + 0 + 1 = 0$ hold.

c. In $\mathbb{Z}_{17}$, we can satisfy $x^2 + y^2 + 1 = 0$ by taking $x = 4$, $y = 0$. This works because in $\mathbb{Z}_{17}$ the equalities $4^2 + 0^2 + 1 = 16 + 0 + 1 = 0$ hold.

d. In $\mathbb{Z}_{29}$, we can satisfy $x^2 + y^2 + 1 = 0$ by taking $x = 12$, $y = 0$. This works because in $\mathbb{Z}_{29}$ the equalities $12^2 + 0^2 + 1 = 144 + 0 + 1 = 145 = 0$ hold. (The fact that $145 = 0$ in $\mathbb{Z}_{29}$ follows by just observing that $29 \times 5 = 145$.)

e. In $\mathbb{Z}_{101}$, we can satisfy $x^2 + y^2 + 1 = 0$ by taking $x = 10$, $y = 0$. This works because in $\mathbb{Z}_{101}$ the equalities $10^2 + 0^2 + 1 = 100 + 0 + 1 = 0$ hold.

f. In $\mathbb{Z}_{103}$, we can satisfy $x^2 + y^2 + 1 = 0$ by taking $x = 13$, $y = 6$. This works because in $\mathbb{Z}_{103}$ the equalities $13^2 + 6^2 + 1 = 169 + 36 + 1 = 206 = 0$ hold.

REMARK 2. Notice that in $\mathbb{Z}_{13}$, $\mathbb{Z}_{17}$, $\mathbb{Z}_{29}$, and $\mathbb{Z}_{101}$ we were able to take $y = 0$. That is, we were able to solve $x^2 + 1 = 0$. This does not contradict Theorem 2, because the four primes p for which we were able to solve $x^2 + 1 = 0$ in $\mathbb{Z}_p$ (that is, $p = 13$, $p = 17$, $p = 29$, $p = 101$) do **not** satisfy the condition that $\frac{p-1}{2}$ is odd, since $\frac{13-1}{2} = 6$, $\frac{17-1}{2} = 8$, $\frac{29-1}{2} = 14$, and $\frac{101-1}{2} = 50$.

S1. Show that in $\mathbb{Z}_4$ the equation $x^2 + y^2 + 1 = 0$ does not have a solution.

Suggested method for S1: Just try all possible values of x and y (there are 4 possibilities for x and 4 for y, so you only have 16 pairs of values to worry about) and verify that in every case the value of $x^2 + y^2 + 1$ is not zero. You can make the argument shorter by observing that the only members of $\mathbb{Z}_4$ that are squares are 0 and 1 (because $0^2 = 0$, $1^2 = 1$, $2^2 = 0$, $3^2 = 1$). So by adding two squares you can only get 0, 1 and 2. You never get 3, which is -1 in $\mathbb{Z}_4$.

A comment about S1: This fact (that $x^2 + y^2 + 1$ never equals 0 in $\mathbb{Z}_4$, that is, that $x^2 + y^2$ never equals 3 in $\mathbb{Z}_4$) has already appeared in the supplementary homework assignment (Problem F), where you were asked to express the number $4,582,623$ as the sum of two squares, with the understanding that the answer could be "it cannot be done." The answer is that $4,582,623$ *cannot be expressed as the sum of two squares*, and the reason is precisely the result of S1: in $\mathbb{Z}_4$, $4,582,623$ is just equal to 3, which is equal to -1, and, as we have proved in S1, you cannot write -1 as a sum $x^2 + y^2$ in $\mathbb{Z}_4$, because if you could then you would have a solution of $x^2 + y^2 + 1 = 0$ in $\mathbb{Z}_4$.

Another comment about S1: S1 shows that **the conclusion of Theorem 1 need not be true if p isn't prime.**

S2. Show that in $\mathbb{Z}_7$ and $\mathbb{Z}_{11}$ the equation $x^2 + 1 = 0$ does not have a solution.

Suggested method for S2: Just compute $x^2 + 1$ in $\mathbb{Z}_7$ for all members x of $\mathbb{Z}_7$ and verify that the result is never 0. Then do the same thing for $\mathbb{Z}_{11}$.

Now, if I was mean, I could ask you to "prove that in $\mathbb{Z}_{103}$ the equation $x^2 + 1$ has no solution." And if I was even meaner, I could ask you to "prove that in $\mathbb{Z}_{1063}$ the equation $x^2 + 1$ has no solution." But if you try to do that by just computing $x^2 + 1$ for all $x \in \mathbb{Z}_{103}$, or by computing $x^2 + 1$ for all $x \in \mathbb{Z}_{1063}$, it is going to be a lot of work!

What you will do, instead, is prove that the equation $x^2 + 1$ has no solution in $\mathbb{Z}_{103}$ or in $\mathbb{Z}_{1063}$ by **reasoning**, *without having to do lots of computations. Furthermore, you will be able to* **explain why** *the equation $x^2 + 1 = 0$ cannot be solved in $\mathbb{Z}_p$ if $p = 7$ or $p = 11$ or $p = 103$ or $p = 1063$.* **The feature that the prime numbers 7, 11, 103 and 1063 have in common is that when you subtract 1 from any of these numbers and then divide by 2 the result is odd.** ($\frac{7-1}{2} = 3$, $\frac{11-1}{2} = 5$, $\frac{103-1}{2} = 51$, and $\frac{1063-1}{2} = 531$.)

Why does this matter? Why does it make such a big difference whether $\frac{p-1}{2}$ is even or odd? Let us find out!!!

S3. Prove: if a, b, p are integers, p is prime, and p divides $a.b$, then p divides a or p divides b.

Suggested method for S3: If p doesn't divide a, then the greatest common divisor of a and p is 1. So we can write 1 as an integer linear combination of a and p. Then multiply both sides by b.
A comment about S3: We did this proof in class. It is also done in the book. I am asking you to write it down anyhow because it is important and I want to

make sure you know it.

S4. Prove: if p is prime and a, b are two nonzero members of $\mathbb{Z}_p$, then $a.b$ is not equal to zero in $\mathbb{Z}_p$.

Suggested method for S4: Use the result of S3.

S5. Prove: the conclusion of S3 need not be true if p is not prime.

Suggested method for S5: find a non-prime p and two nonzero members of $\mathbb{Z}_p$ such that $a.b = 0$ in $\mathbb{Z}_p$.

S6. Prove: if p is a prime number such that $p \neq 2$ and a is a member of $\mathbb{Z}_p$ such that $a \neq 0$ and there exists an $x \in \mathbb{Z}_p$ for which $x^2 = a$, then there exist exactly two values of $x \in \mathbb{Z}_p$ such that $x^2 = a$.

An example, to illustrate and clarify S6: Suppose we take $p = 11$, $a = 3$. Then the equation $x^2 = a$ has a solution, because we can take $x = 5$, which gives $x^2 = 25 = 3$ in $\mathbb{Z}_{11}$. If the result of S6 is true, then there ought to be another solution, and indeed there is, because $x = 6$ is also a solution, since $6^2 = 36 = 3$ in $\mathbb{Z}_{11}$. Furthermore, if the result of S6 is true, then there ought to be no other solutions besides $x = 5$ and $x = 6$. And indeed there aren't any other solutions. (You can verify this by computing x^2 for all 11 possible values of $x \in \mathbb{Z}_{11}$, and you will see that the only values for which $x^2 = 3$ are 5 and 6.)

Suggested method for S6: Suppose there is an x such that $x^2 = a$. Pick one and call it ξ. Then show that $-\xi$ is also a solution, and *prove that $-\xi$ is not equal to ξ in $\mathbb{Z}_p$.* (See the remark below for the meaning of $-\xi$.) Finally (and this is the hardest part), we have to prove that ξ and $-\xi$ are the only solutions, that is, that if η is any solution then $\eta = \xi$ or $\eta = -\xi$. To prove this, observe that if $\eta^2 = a$ then $\eta^2 = \xi^2$, because $\xi^2 = a$. So $\eta^2 - \xi^2 = 0$. So $(\eta - \xi)(\eta + \xi) = 0$. And now comes the key step: *thanks to S4, the equality $(\eta - \xi)(\eta + \xi) = 0$ implies that $\eta - \xi = 0$ or $\eta + \xi = 0$.* So $\eta = \xi$ or $\eta = -\xi$.

REMARK 3. Recall what "$-x$" means in $\mathbb{Z}_n$. If $x \in \mathbb{Z}_n$, then $-x$ is the member y of $\mathbb{Z}_n$ such that $x + y = 0$. For example, in $\mathbb{Z}_{13}$, we have $-3 = 8$ and $-7 = 4$.

S7. Prove: if $p = 2$ then the conclusion of S6 need not be true.

Suggested method for S7: Pick an $a \in \mathbb{Z}_2$ such that $a \neq 0$ (you don't have that many choices for a) and count how many values of $x \in \mathbb{Z}_2$ there are for which $x^2 = a$.

S8. Where in your proof of S6 was the fact that $p \neq 2$ used?

Suggested method for S8: Think.

S9. Prove that if p isn't prime then the conclusion of S6 need not be true.

Suggested method for S9: How many values are there of $x \in \mathbb{Z}_{12}$ such that $x^2 = 4$ in $\mathbb{Z}_{12}$?

S10. Where in your proof of S6 was the fact that p is prime used?

Suggested method for S10: Think.

S11. Prove that if $a = 0$ then the conclusion of S6 need not be true.

Suggested method for S11: How many values are there of $x \in \mathbb{Z}_7$ such that $x^2 = 0$ in $\mathbb{Z}_7$?

S12. Where in your proof of S6 was the fact that $a \neq 0$ used?

Suggested method for S12: Think.

Now, if n is an integer such that $n > 1$, we introduce the notation $\mathbb{Z}_n^*$ to stand for the set of *nonzero* members of $\mathbb{Z}_n$. So, for example,

$$\begin{aligned}
\mathbb{Z}_2^* &= \{1\}\,, \\
\mathbb{Z}_3^* &= \{1,2\}\,, \\
\mathbb{Z}_4^* &= \{1,2,3\}\,, \\
&\vdots \\
\mathbb{Z}_{10}^* &= \{1,2,3,4,5,6,7,8,9\}\,, \\
&\vdots \\
\mathbb{Z}_{17}^* &= \{1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16\}\,, \\
&\vdots
\end{aligned}$$

It is then obvious that

$$|\mathbb{Z}_n^*| = n - 1\,,$$

that is, that **the set $\mathbb{Z}_n^*$ has $n - 1$ members**.

We then define a function $\Phi_n : \mathbb{Z}_n^* \mapsto \mathbb{Z}_n$ by letting

$$\Phi_n(x) = x^2 \quad \text{if} \quad x \in \mathbb{Z}_n^*\,.$$

(Here, of course, "x^2" means "the square of x in $\mathbb{Z}_n$." For example, $\Phi_7(4) = 2$, because $4^2 = 16 = 2$ in $\mathbb{Z}_7$.)

Also, we define a relation E_n on $\mathbb{Z}_n^*$ as follows:

$$E_n = \{(x,y) \in \mathbb{Z}_n^* \times \mathbb{Z}_n^* : \Phi_n(x) = \Phi_n(y)\}\,.$$

(That is, if x and y belong to $\mathbb{Z}_n^*$, then xE_ny if and only if $x^2 = y^2$ in $\mathbb{Z}_n$.)

S13. Prove: if p is prime then $\Phi_p : \mathbb{Z}_p^* \mapsto \mathbb{Z}_p^*$.

Suggested method for S13: Use S4.

S14. Prove: if n is a positive integer then E_n is an equivalence relation on $\mathbb{Z}_n^*$.

Suggested method for S14: No suggestions, because this is very easy.

S15. Prove: if p is prime and $p > 2$ then every E_p-equivalence class has exactly two members.

Suggested method for S15: Use S6.

S16. Prove: if p is prime and $p > 2$ then the number of E_p-equivalence classes is $\frac{p-1}{2}$

Suggested method for S16: Use Theorem 13.6, page 92.

We let $\mathcal{P}_n$ be the set of equivalence classes of E_n. We let $\mathcal{S}_n$ be the set of members of $\mathbb{Z}_n$ that are squares (in $\mathbb{Z}_n$) of members of $\mathbb{Z}_n^*$.

EXAMPLES:

$$\begin{aligned}
\mathcal{P}_7 &= \Big\{ \{1,6\}, \{2,5\}, \{3,4\} \Big\}, \\
\mathcal{S}_7 &= \{1,2,4\}, \\
\mathcal{P}_8 &= \Big\{ \{1,3,5,7\}, \{2,6\}, \{4\} \Big\}, \\
\mathcal{S}_8 &= \{0,1,4\}, \\
\mathcal{P}_{13} &= \Big\{ \{1,12\}, \{2,11\}, \{3,10\}, \{4,9\}, \{5,8\}, \{6,7\} \Big\}, \\
\mathcal{S}_{13} &= \{1,3,4,9,10,12\}.
\end{aligned}$$

We define a function $\Psi_n : \mathcal{S}_n \mapsto 2^{\mathbb{Z}_n^*}$ by letting

$$\Psi_n(s) = \{x \in \mathbb{Z}_n^* : x^2 = s\} \qquad \text{if} \qquad s \in \mathcal{S}_n.$$

EXAMPLES:

$$\begin{aligned}
\Psi_7(1) &= \{1,6\}, \\
\Psi_7(2) &= \{3,4\}, \\
\Psi_7(4) &= \{2,5\}, \\
\Psi_8(0) &= \{4\}, \\
\Psi_8(1) &= \{1,3,5,7\}, \\
\Psi_8(4) &= \{2,6\}.
\end{aligned}$$

S17. Prove: if p is prime and $p > 2$ then

a. $\Psi_p : \mathcal{S}_n \mapsto \mathcal{P}_p$,

b. Ψ_p is one-to-one,

c. Ψ_p is onto $\mathcal{P}_p$.

S18. Prove: if p is prime and $p > 2$ then $|\mathcal{S}_p| = \frac{p-1}{2}$. (In other words, the number of squares in $\mathbb{Z}_p^*$ is exactly $\frac{p-1}{2}$.)

We now write $\mathcal{NS}_n$ to denote the set $\mathbb{Z}_n^* - \mathcal{S}_n$. That is, $\mathcal{NS}_n$ is the set of nonzero members of $\mathbb{Z}_n$ that are *not* squares.

S19. Prove: if p is prime and $p > 2$ then $|\mathcal{NS}_p| = \frac{p-1}{2}$. (In other words, the number of non-squares in $\mathbb{Z}_p^*$ is exactly $\frac{p-1}{2}$.)

Statements S18 and S19 say that *exactly half* the members of $\mathbb{Z}_p^*$ are squares. So the set $\mathbb{Z}_p^*$ is divided into two sets of equal size: the squares and the non-squares.

EXAMPLES:

a. Of the twelve members $\mathbb{Z}_{13}^*$, the following six are squares: 1,3,4,9,10,12. The other six are not squares.

b. Without computing anything, we can be sure that of the 100 members of $\mathbb{Z}_{101}^*$ (i) 50 are squares, and (ii) the other 50 are not squares.

c. Without computing anything, we can be sure that of the 102 members of $\mathbb{Z}_{103}^*$ (i) 51 are squares, and (ii) the other 51 are not squares.

S20. Prove: if p is prime and $a \in \mathbb{Z}_p^*$, then there exists $b \in \mathbb{Z}_p$ such that $a.b = 1$ in $\mathbb{Z}_p$.

Suggested method for S20: The gcd of a and p has to be 1. Write 1 as an integer linear combination of a and p, and see what that says modulo p.

S21. Prove: if p is prime and $a, b \in \mathcal{NS}_p$, then there exists $c \in \mathbb{Z}_p^*$ such that $a.c^2 = b$.

Suggested method for S21: Fix a. Define a function $G : \mathcal{S}_p \mapsto \mathbb{Z}_p$ by letting $G(x) = a.x$. Then prove that G is one-to-one. (Hint: if $G(x) = G(x')$, then $a.x = a.x'$, so $a.x - a.x' = 0$, so $a.(x - x') = 0$. Since $a \neq 0$, we can pick b such that $b.a = 1$. Then $x - x' = 1.(x - x') = b.a.(x - x') = b.0 = 0$, so $x = x'$.) Next, prove that $G : \mathcal{S}_p \mapsto \mathcal{NS}_p$. (Hint: Suppose $x \in \mathcal{S}_p$, and $y = G(x)$. Write $x = z^2$, $z \in \mathbb{Z}_p^*$. Then $y = z^2.a$. Since $a \neq 0$ and $z \neq 0$, S4—applied twice—implies $y \neq 0$, so $y \in \mathbb{Z}_p^*$. If y was a square, say $y = u^2$, then we would have $u^2 = z^2 a$. Using $S20$, pick v such that $z.v = 1$. Then $a = 1.a = z.v.z.v.a = z^2 a.v^2 = u^2 v^2 = (u.v)^2$, so a would be a square. Therefore y is not a square.) Finally, since we now know that $G : \mathcal{S}_p \mapsto \mathcal{NS}_p$ is one-to-one, and S18 and S19 imply that $|\mathcal{S}_p| = |\mathcal{NS}_p|$, then Problem 20.11 (page 170) implies that G is onto. Therefore there exists $s \in \mathcal{S}_p$ such that $G(s) = b$. Write $s = c^2$, $c \in \mathbb{Z}_p^*$.

S22. Prove: if p is prime and $a \in \mathcal{NS}_p$, then there exist $x, y \in \mathbb{Z}_p$ such that $x^2 + y^2 = a$.

Suggested method for S22: There are two possibilities. Either

I. $\forall x \in \mathbb{Z}_p, \forall y \in \mathbb{Z}_p, x^2 + y^2 \in \mathcal{S}_p \cup \{0\}$

or

II. $\exists x \in \mathbb{Z}_p, \exists y \in \mathbb{Z}_p, x^2 + y^2 \notin \mathcal{S}_p \cup \{0\}$.

If I holds, then "the sum of two squares in $\mathbb{Z}_p$ is a square in $\mathbb{Z}_p$." Then, since 1 is a square, we can conclude that $1+1$ is a square, so 2 is a square. Then $3 = 2+1$ is a square, $4 = 3+1$ is a square, and so on. To make this "and so on" precise, prove by induction (or well ordering) that every member of $\mathbb{Z}_p$ is a square. In particular, a is a square, contradicting our hypothesis that $a \in \mathcal{NS}_p$. Hence Case I cannot occur. So we must be in Case II. This means that we can pick $u, v \in \mathbb{Z}_p$ such that $b = u^2 + v^2$ is not a square. Then by S21 we can write $a = b.c^2$ for some $c \in \mathbb{Z}_p$. Therefore $a = (u^2+v^2).c^2 = (u.c)^2 + (v.c)^2$, so a is the sum of two squares.

S23. Prove Theorem 1.

Suggested method for S23: If -1 is a square in $\mathbb{Z}_p$, then $-1 = x^2$ for some x, so x^2+1, and we can find a solution of $x^2+y^2+1 = 0$ by just taking $y = 0$. If -1 is not a square in $\mathbb{Z}_p$, then S22 tells us that -1 is the sum of two squares, so $-1 = x^2+y^2$ for some x, y, and then $x^2+y^2+1 = 0$.

Now define a function $\Theta : \mathcal{S}_p \mapsto \mathbb{Z}_p$ by letting $\Theta(x) = x^2$. Then define a relation H on $\mathcal{S}_p$ by letting xHy if and only if $\Theta(x) = \Theta(y)$.

S24. Prove: if p is prime, then H is an equivalence relation on $\mathcal{S}_p$.

S25. Prove: if p is prime and $p \neq 2$, and $-1 \in \mathcal{S}_p$, then every equivalence class of H has exactly two members.

S26. Prove: if p is prime and $p \neq 2$, and $-1 \in \mathcal{S}_p$, then $\frac{p-1}{2}$ is even.

Suggested method for S26: Use S25 and S18. Since $\mathcal{S}_p$ has $\frac{p-1}{2}$ members, and $\mathcal{S}_p$ is partitioned into equivalence classes having two members each, the number of equivalence classes must be $\frac{1}{2}\left(\frac{p-1}{2}\right)$. So $\frac{1}{2}\left(\frac{p-1}{2}\right)$ must be an integer.

S27. Prove Theorem 2.

Suggested method for S27: If we can solve $x^2+1 = 0$, then $-1 \in \mathcal{S}_p$, so S26 tells us that $\frac{p-1}{2}$ cannot be odd.

A CONCLUDING REMARK. Theorem 2 provides an incomplete answer to the natural question: *For which primes p is it possible to solve $x^2+1 = 0$ in $\mathbb{Z}_p$?* The theorem says that the equation x^2+1 cannot be solved if $p \neq 2$ and $\frac{p-1}{2}$ is odd. But the question remains: *can the equation always be solved if $\frac{p-1}{2}$ is even?* In the specific examples we looked at ($p = 13$, $p = 17$, $p = 29$, $p = 101$) the answer was "yes." But this, of course, does not guarantee that the answer is always yes. The following theorem answers the question:

THEOREM 3. *Let p be a prime number such that $p \neq 2$ and $\frac{p-1}{2}$ is even. Then the equation $x^2+1 = 0$ has a solution in $\mathbb{Z}_p$. (That is, there exists an $x \in \mathbb{Z}_p$ such that $x^2+1 = 0$ in $\mathbb{Z}_p$.)*

This theorem is true, but we will not prove it because it is a little bit too hard for this course.