**MATH 371 – Class notes/outline – September 24, 2013**

**Rings**

Armed with what we have looked at for the integers and polynomials over a field, we're in a good position to take up the general theory of rings.

**Definitions**: A *ring* is an abelian group $(R, +)$ with an additional binary operation called multiplication. For every $x, y, z \in R$:

1. $(x \cdot y) \cdot z = x \cdot (y \cdot z)$
2. There exists an element $1 \in R$ such that $1 \cdot x = x \cdot 1 = x$
3. $x \cdot (y + z) = x \cdot y + x \cdot z$ and $(y + z) \cdot x = y \cdot x + z \cdot x$.

(the identity for addition in $R$ is denoted 0, and we'll usually leave out the dot in $x \cdot y$).

A set $S \subset R$ is called a *subring* of $R$ if $S$ is a subgroup of $(R, +)$, $1 \in S$ and $xy \in S$ if $x, y \in S$.

An element $x \in R$ is called a *zero divisor* if there exists $y \in R$ with $y \neq 0$ but $xy = 0$ or $yx = 0$.

An element $x \in R$ is called a *unit* if there exists $y \in R$ such that $xy = yx = 1$. Then we write $y = x^{-1}$. The set of units in $R$ is denoted $R^*$.

$R$ is called a *commutative ring* if $xy = yx$ for all $x, y \in R$.

**Examples**: Commutative rings: $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $k[x_1, \ldots, x_n]$, $R[x_1, \ldots, x_n]$.
Non-commutative rings: $n \times n$ matrices (with coefficients in a commutative ring) for $n \geqslant 2$, quaternions $\mathbb{H}$.

**We will stick to commutative rings from here out, unless otherwise stipulated!!**

**More definitions**: A *field* is a ring with $R^* = \{r \in R \mid r \neq 0\}$ If $K \subset L$ are fields and $K$ is a subring of $L$ then $K$ is called a *subfield* of $L$ and $L$ is called an *extension field* of $K$.

An *integral domain* (or sometimes just "domain") is a ring with no zero divisors.

**Proposition**: In an integral domain $R$, suppose $a, x, y \in R$ with $a \neq 0$. If $ax = ay$ then $x = y$ (this is called *cancellation*).

Let $F$ be a field. Then $F$ is an integral domain.

**Example**: The set $\mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\} \subset \mathbb{C}$ is a subring of $\mathbb{C}$. In fact, $\mathbb{Q}(i)$ is a field so $\mathbb{Q}(i)$ is a subfield of $\mathbb{C}$. In algebra, if $z = a + bi \in \mathbb{C}$, it is common to call $|z|^2 = a^2 + b^2$ the *norm* of $z$ and to denote it $N(z)$. Note that $N(z_1 z_2) = N(z_1)N(z_2)$.

Within $\mathbb{Q}(i)$ there is the subring $\mathbb{Z}[i]$ of *Gaussian integers*. The norm $N(z)$ of a Gaussian integer $z \in \mathbb{Z}[i]$ must be a non-negative integer, and then the multiplicative property of the norm implies that $z \in \mathbb{Z}[i]$ is a unit of $\mathbb{Z}[i]$ if and only if $N(z) = 1$ (Proof?). This yields $\mathbb{Z}[i]^* = \{\pm 1, \pm i\}$. Note that prime numbers in $\mathbb{Z}$ are not necessarily "prime" in $\mathbb{Z}[i]$, e.g., $5 = (2+i)(2-i)$. More on this phenomenon later.

**Ideals**: Just as we defined ideals in $k[x_1, \ldots, x_n]$, we can define ideals in any ring. An *ideal* in $R$ is a subgroup $I$ of $(R, +)$ such that $rx \in I$ for every $a \in R$ and $x \in I$. Note: $R$ is an ideal of itself, and $I = R$ if and only if $1 \in I$. For $r_1, \ldots, r_s \in R$ we can define

$$\langle r_1, \ldots, r_s \rangle = \{a_1 r_1 + \cdots + a_s r_s \,|\, a_1, \ldots, a_s \in R\}$$

to be the ideal generated by $r_1, \ldots, r_s$. If an ideal is generated by a finite set, it is called finitely generated. You can also talk about ideals generated by infinite sets (the sums are still finite, but the set from which the $r$'s are chosen can be infinite).

If $I$ and $J$ are ideals in $R$, then $I \cap J$ and $I + J = \{i + j \,|\, i \in I, \, j \in J\}$ are also ideals in $R$. The product $IJ$ is defined to be the ideal generated by $\{ij \,|\, i \in I, \, j \in J\}$. Note that $IJ \subset I \cap J$.

The only ideals of a field $F$ are $\{0\}$ and $F$ itself.

An ideal generated by one element $\langle r \rangle$ is called a *principal ideal*. If $R$ is an integral domain, and every ideal of $R$ is principal then $R$ is called a *principal ideal domain*. We know that $\mathbb{Z}$ and $k[x]$ (polynomials in one variable over a field) are principal ideal domains. Perhaps surprising:

**Theorem**: The ring of Gaussian integers $\mathbb{Z}[i]$ is a principal ideal domain.

(Idea of proof: If $I$ is a non-zero ideal in $\mathbb{Z}[i]$, then let $d \in I$ have minimal norm. For any $z \in I$ consider $z/d$ (in $\mathbb{Q}(i)$), and let $q \in \mathbb{Z}[i]$ with $N(q - z/d) < 1$. Multiply this by $N(d)$ to see that $N(qd - z) < N(d)$ but $qz - d \in I$, a contradiction unless $d = qz$.)

For the record, $k[x, y]$, $\mathbb{Z}[x]$ and $\mathbb{Z}[\sqrt{-5}]$ are not principal ideal domains.

**Quotient rings**: If $I$ is an ideal of $R$, then the set $R/I = \{[x] \,|\, x \in R\}$ of (left) cosets $[x] = x + I$ of $I$ (thinking of $I$ as a subgroup of the abelian group $(R, +)$) can be made into a ring in the obvious way (recall $[x] = [y]$ means $x - y \in I$): $[x] + [y] = [x + y]$ and $[x][y] = [xy]$ for all $[x], [y] \in R/I$. This new ring is called the *quotient ring* of $R$ by $I$. Note $[0]$ is the additive identity and $[1]$ the multiplicative identity in $R/I$, and $[x] = [0]$ if and only if $x \in I$.

We've already met the quotient rings $\mathbb{Z}/\langle d \rangle$ – this is a field if and only if $d$ is prime and otherwise has zero divisors (unless $d = 0$ in which case you still have $\mathbb{Z}$). If $p$ is a prime number, we'll write $\mathbb{F}_p$ for the field $\mathbb{Z}/\langle p \rangle$.

**Prime and maximal ideals**: By analogy with the basic property of prime numbers, namely that if $p \mid ab$ then either $p \mid a$ or $p \mid b$, we define a *prime ideal* $I \subset R$ to be an ideal such that if $xy \in I$ then either $x \in I$ or $y \in I$ (or both). If $I$ is a prime ideal and $I \neq R$ then $R/I$ is an integral domain (and conversely).

A *maximal ideal* is one not properly contained in any other proper ideal, i.e., $I$ is maximal if for any other ideal $J$, the containment $I \subset J$ implies that either $J = I$ or $J = R$. An ideal $I \subset R$ is maximal if and only if $R/I$ is a field.

**Homomorphisms of rings**: A mapping $f\colon R \to S$ from one ring to another is called a *homomorphism* (or, more precisely, a ring homomorphism) if it is a group homomorphism from $(R, +)$

to $(S, +)$ (i.e., if $f(x+y) = f(x) + f(y)$ for all $x, y \in R$) and if $f(xy) = f(x)f(y)$ for all $x, y \in R$. It's called an isomorphism if it's a bijection (and so is invertible), and then $R$ and $S$ are isomorphic (denoted $R \cong S$).

The map $R \to R/I$ given by $x \mapsto [x]$ is the canonical example of a ring homomorphism (it's surjective but not injective unless $I = \{0\}$).

The kernel $\ker(f) = \{r \in R \,|\, f(r) = 0\}$ of a ring homomorphism is an ideal of $R$ and the image is a subring of $S$. The standard isomorphism theorem is almost immediate, that if $f\colon R \to S$ is a homomorphism with $\ker(f) = K$, then $\overline{f}\colon R/K \to f(R)$ (where $\overline{f}(r + K) = f(r)$ is well-defined and an isomorphism.

For every ring $R$ there is a unique homomorphism $f\colon \mathbb{Z} \to R$. Using this homomorphism one can define $nr$ for $n \in \mathbb{Z}$ and $r \in R$ as $nr = f(n)r = r + r + \cdots + r$ ($n$ times). The generator of the kernel of this homomorphism is the *characteristic* of the ring $R$. If $R$ is an integral domain, then this generator is a prime number. If moreover $R$ is finite then it is a field.

The binomial theorem is true in any ring:

$$(a+b)^n = a^n + \binom{n}{1} a^{n-1}b + \cdots + \binom{n}{n-1} ab^{n-1} + b^n$$

for $n \in \mathbb{N}$ (proof by induction). From this get the "freshman's dream": In a ring $R$ of prime characteristic $p$, we have

$$(x+y)^{p^e} = x^{p^e} + y^{p^e}$$

for all $x, y \in R$ and $e \in \mathbb{N}$. (Induct on $e$ and use that $p \mid \binom{p}{i}$ for $1 \leqslant i \leqslant p-1$ from homework 1). Use this to show that the "Frobenius map" $F\colon R \to R$ given by $F(x) = x^p$ is a ring homomorphism.

**Fraction field of an integral domain**: Just as you make $\mathbb{Q}$ from $\mathbb{Z}$, given any integral domain $R$ you can make a natural field $Q$ containing $R$, such that $Q$ is the smallest field containing $R$ (in the sense that if $F$ is any other field and there is an injective homomorphism $R \to F$, then there is an injective homomorphism $Q \to F$ which extends it.) $Q$ comprises equivalence classes of symbols $r/s$ for $r, s \in R$ with $s \neq 0$ where $r/s \sim r'/s'$ means that $rs' = r's$. And so it goes.

For instance, the field of fractions of $\mathbb{Z}[i]$ is $\mathbb{Q}(i)$.

**Factorization**

In the integers and polynomials over a field, the ideas of divisibility and factorization are important. These led to the notion of prime numbers and irreducible polynomials. We generalize these ideas here to arbitrary *integral domains*. So from here out in these notes, we'll assume all our rings are integral domains (so that in particular, the cancellation law holds).

**Definitions**: Let $R$ be an integral domain. For $x, y \in R$, say $y$ divides $x$, write $y \mid x$ if $x = ry$ for some $r \in R$. We have $y \mid x$ if and only if $\langle x \rangle \subset \langle y \rangle$. We'll have $\langle x \rangle = \langle y \rangle$ if and only if $r \in R^*$, in which case we say $x$ and $y$ are *associates* in $R$.

The element $d \in R$ is called a *greatest common divisor* of $a, b \in R$ if $d \mid a$ and $d \mid b$ and for any other $x$ which divides both $a$ and $b$, we have $x \mid d$ as well. If $R$ is a principal ideal domain, then $\langle a, b \rangle = \langle d \rangle$ for some $d$ and $d$ is a greatest common divisor of $a$ and $b$ (Proof?).

A non-unit $r$ in $R$ is called *irreducible* if $r = ab$ for $a, b \in R$ implies that either $a$ or $b$ is a unit. A non-zero non-unit $x \in R$ is said to have a *factorization into irreducible elements* if there are irreducibles $p_1, \ldots, p_r \in R$ such that $x = p_1 \cdots p_r$ And $x$ is said to have *unique factorization into irreducible elements* if for any other irreducible factorization $x = q_1 \cdots q_s$ we have that every $p_i$ for $i = 1, \ldots, r$ divides $q_j$ for some $j = 1, \ldots, s$ (which implies that $q_j = up_i$ where $u$ is a unit). In particular, $r = s$. A domain $R$ such that every non-zero non-unit has unique factorization into irreducible elements is called a *unique factorization domain.*

A non-zero non-unit $p$ in $R$ is called a *prime element* if $p \mid xy$ for $x, y \in R$ implies that either $p \mid x$ or $p \mid y$.

**Proposition**. A prime element is irreducible.

(Idea of proof): If $p$ is prime and $p = ab$, then either $p \mid a$ or $p \mid b$. If $p \mid a$ then $a = rp$, but then $p = rpb$. Cancelling the $p$'s shows that $b$ is a unit, so $p$ is irreducible.

**Proposition**: Let $R$ be a domain for which every non-zero non-unit has a factorization into irreducibles. Every irreducible element is prime if and only if $R$ is a unique factorization domain.

(Idea of proof): ($\Rightarrow$) If $x$ has two irreducible factorizations $x = p_1 \cdots p_r = q_1 \cdots q_s$ then each $p_i$ must divide some $q_j$ and vice versa because they're also prime. ($\Leftarrow$) Suppose $x$ is irreducible and $x \mid ab$. Then $ab = xr$, factor both sides into irreducibles (on the right, do this by factoring $r$ into irreducibles, on the left do this by factoring $a$ and $b$ into irreducibles) – by uniqueness $x$ must be an associate of one of the factors on the left, which is a factor of either $a$ or $b$, so $x$ is prime.

**Example**: In $R = \mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$, the number 2 is irreducible but not prime. See this because there are two irreducible factorizations of $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$. (Use the norm function $N(a + b\sqrt{-5}) = a^2 + 5b^2$ to conclude that $\mathbb{Z}[\sqrt{-5}]^* = \{\pm 1\}$ and that the four factors are irreducible).

Our goal now is to show that if $R$ is a principal ideal domain, then $R$ is also a unique factorization domain.

**Lemma**: Let $R$ be a principal ideal domain and $x \in R$ a non-zero element. Then $x$ has an irreducible factorization.

(Idea of proof): If $x$ is irreducible then we're done. If not, factor $x = p_1 q_1$ where neither $p_1$ nor $q_1$ is a unit. But then $\langle x \rangle \subsetneq \langle p_1 \rangle$ and $\langle x \rangle \subsetneq \langle q_1 \rangle$. If one of $p_1, q_1$ is not irreducible we can further factor. This process cannot go on forever since you can't have an infinite increasing sequence of ideals in a principal ideal domain (Proof?), and it will terminate in an irreducible factorization of $x$.

**Proposition**: Let $R$ be a principal ideal domain that is not a field. An ideal $\langle x \rangle \subset R$ is a maximal ideal if and only if $x$ is irreducible.

*Proof.* If $x$ is irreducible and $\langle x \rangle \subset \langle y \rangle$, then $x = sy$, but then $s$ must be a unit. Thus $\langle x \rangle = \langle y \rangle$ or $\langle y \rangle = R$, so $\langle x \rangle$ is a maximal ideal. On the other hand, if $\langle x \rangle$ is maximal and $x = sy$ then one of $s, y$ must be a unit, otherwise $\langle x \rangle \subsetneq \langle y \rangle \subsetneq R$, contradicting that $\langle x \rangle$ is maximal.

**Theorem**. A principal ideal domain $R$ is a unique factorization domain.

*Proof.* From the lemma above, we know that every non-zero element in $R$ has a factorization, so we only have to prove uniqueness. We'll apply one of the propositions above and show that every irreducible element is prime. So let $p \in R$ be irreducible and suppose $p \mid ab$ but $p \nmid a$. Then $a \notin \langle p \rangle$ therefore $\langle a, p \rangle \supsetneq \langle p \rangle$. Since $\langle p \rangle$ is maximal by the proposition immediately above, we have $\langle a, p \rangle = R = \langle 1 \rangle$. Therefore there are $\lambda, \mu \in R$ such that $\lambda a + \mu p = 1$, therefore $\lambda ab + \mu bp = b$. But we know that $p \mid ab$ therefore $p \mid b$, and so $p$ is prime, and we're done. (Doesn't this proof look familiar? See the proof of corollary 1 on page 3 of the notes on integers.)

**Examples**: The ring $\mathbb{Z}[\sqrt{-5}]$ is not a principal ideal domain since 2 is an irreducible element that is not prime. In fact $I = \langle 2, 1 + \sqrt{-5} \rangle$ is not a principal ideal — if $x \in I$ then $x = (2a + b) + b\sqrt{- - 5}$ for $a, b \in \mathbb{Z}$ and use the norm function from before.

The ring of Gaussian integers $\mathbb{Z}[i]$, being a principal ideal domain, is a unique factorization domain.

One more task before we leave the realm of factorization for a bit: In which rings (integral domains) can we use the Euclidean algorithm (rather than factoring) to find greatest common divisors? The answer is that we have to have a version of the division algorithm so that for every $x, d \in R$ with $d \neq 0$ there exist $q, r \in R$ such that $x = qd + r$ and $r$ is "smaller" than $d$ in some sense.

**Definition**: A *Euclidean domain* $R$ is an integral domain on which there is a function $N$ that maps the nonzero elements of $R$ to the non-negative integers and which satisfies: for every $x, d \in R$ with $d \neq 0$ there exist $q, r \in R$ such that $x = qd + r$ with either $r = 0$ or $N(r) < N(d)$.

So the integers (with $N$ the absolute value function), polynomials in one variable over a field (with $N$ the degree function) and the Gaussian integers (with $N$ the norm function) are all Euclidean domains. Mimic the proof of the fact that the ring of Gaussian integers is a principal ideal domain (on page 2) to get

**Theorem**: A Euclidean domain $R$ is a principal ideal domain (hence a unique factorization domain).

And once you have the division algorithm, the Euclidean algorithm follows.

There are principal ideal domains that are not Euclidean domains. $\mathbb{Z}[(1 + \sqrt{-19})/2]$ is one such, but that is not so easy to prove.

**The Gaussian integers and number theory**

The theorem on page 2 shows that the ring of Gaussian integers $\mathbb{Z}[i]$ is a Euclidean domain where the function $N$ is the norm function as we defined it there: $N(a + bi) = a^2 + b^2$. So the Gaussian integers are a unique factorization domain. It is interesting to ask what are the primes in $\mathbb{Z}[i]$, and to start with asking what happens to the ordinary integer primes.

**Proposition**: If $z \in \mathbb{Z}[i]$ is a Gaussian integer such that $N(z) = p$ and $p$ is a prime number, then $z$ is a prime element of $\mathbb{Z}[i]$.

*Idea of proof*: Since primes and irreducibles are the same in a UFD, we'll show that $z$ is irreducible. If $z = ab$ then $N(z) = N(a)N(b)$, so one of $N(a)$ and $N(b)$ has to be 1 and the other $p$. But the one with norm 1 is a unit, so $z$ is irreducible.

Now we know that some prime numbers like $5 = (2+i)(2-i)$ and $13 = (3+2i)(3-2i)$ become reducible in $\mathbb{Z}[i]$. We examine this phenomenon a little more closely.

**Lemma** (Lagrange): Let $p$ be a prime number (i.e., a prime *integer*). If $p \equiv 1 \pmod 4$ then the congruence

$$x^2 \equiv -1 \pmod p$$

has a solution.

*Proof*: In fact, writing $p = 4n+1$ we can take $x = (2n)!$. Use Wilson's theorem (problem 9(b) on Homework 1), which tells us that $(p-1)! = (4n)! \equiv -1 \pmod p$. But

$$(4n)! = (4n)(4n-1)(4n-2)\cdots(4n-2n+1)(2n)(2n-1)\cdots 3\cdot 2\cdot 1$$

and we note that $4n \equiv -1 \pmod p$, $4n-1 \equiv -2 \pmod p$,...,$(4n-2n+1) \equiv -2n \pmod p$ so it follows that $((2n)!)^2 \equiv (4n)! \equiv -1 \pmod p$.

**Corollary**. A prime number $p \equiv 1 \pmod 4$ is not prime in $\mathbb{Z}[i]$.

Because there's an $x$ such that $x^2+1 \equiv 0 \pmod p$, i.e., $p \mid x^2+1 = (x+i)(x-i)$. But $p \nmid x+i$ and $p \nmid x-i$, since $x/p \pm (1/p)i \notin \mathbb{Z}[i]$.

This leads to a famous theorem of Fermat:

**Fermat's two-square theorem**: A prime number $p \equiv 1 \pmod 4$ is the sum of two uniquely determined squares.

*Proof.* (Uniqueness) Suppose $p = a^2+b^2$. Then $p = (a+bi)(a-bi)$ in $\mathbb{Z}[i]$ and since $N(a \pm bi) = a^2+b^2 = p$ is prime, but the proposition above we have that $a \pm bi$ is irreducible. Now suppose also $p = c^2+d^2$. Therefore $p = (c+di)(c-di)$ is *another* irreducible factorization of $p$. Since $\mathbb{Z}[i]$ is a UFD, we must have that $c+di$ is a unit times either $a+bi$ or $a-bi$, and similarly for $c-di$. But the units of $\mathbb{Z}[i]$ are $\pm1, \pm i$, so we must have $\{a^2, b^2\} = \{c^2, d^2\}$.

(Existence) From the corollary above, we know that $p$ is not prime in $\mathbb{Z}[i]$, so write $p = yz$ where $y = a+bi$ is prime in $\mathbb{Z}[i]$. We can't have $z$ a unit, or else $p$ would be prime, so $N(z) > 1$. But $N(p) = p^2$ so the only choice is $N(z) = p$ and $N(y) = p$. But $N(y) = a^2+b^2$ so we have expressed $p = a^2+b^2$.

Note that this proof doesn't tell us how to *find* $a$ and $b$ so that $a^2+b^2 = p$. There is an algorithm for this, but before we can present it, we need to digress a bit on quadratic residues — this has to do with whether one can solve the equation $x^2 = a \pmod p$ for various numbers $a$.

**Definition**: Let $p$ be a prime number. If $p \nmid a$ then $a$ is called a *quadratic residue* modulo $p$ if there exists $x \in \mathbb{Z}$ such that $a \equiv x^2 \pmod p$. Otherwise, $a$ is called a *quadratic non-residue* modulo $p$. If $p \mid a$ then $a$ is considered neither a quadratic residue nor a quadratic non-residue. This definition is encapsulated in the *Legendre symbol*:

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } p \mid a \\ 1 & \text{if } a \text{ is a quadratic residue modulo } p \\ -1 & \text{if } a \text{ is a quadratic non-residue modulo } p. \end{cases}$$

By thinking in the ring $\mathbb{Z}/\langle p\rangle$, we see that if $a \equiv x^2 \pmod{p}$ for some integer $x \in \mathbb{Z}$, then there is a $y$ such that $0 \leqslant y < p$ with $a \equiv y^2 \pmod{p}$. Therefore the quadratic residues in $(\mathbb{Z}/\langle p\rangle)^*$ are the numbers $[1^2], [2^2], \ldots, [p-1]^2$, where the brackets mean mod $p$. This tells us that the Legendre symbol satisfies

$$\left(\frac{a}{p}\right) = \left(\frac{a+kp}{p}\right)$$

for any $k \in \mathbb{Z}$.

A little experimenting will convince you that the following proposition ought to be true:

**Proposition**: If $p$ is an odd prime then half the numbers $1, 2, \ldots, p-1$ are quadratic residues, while the other half are quadratic non-residues mod $p$.

*Proof.* Since $x^2 \equiv (p-x)^2 \pmod{p}$, the quadratic residues mod $p$ are actually given by the first $(p-1)/2$ squares $[1^2], [2^2], \ldots, [((p-1)/2)^2]$. And these numbers are different, since if $[i^2] = [j^2]$ we have $p \mid (i^2 - j^2) = (i+j)(i-j)$. But $p$ cannot divide $i+j$ if $0 < i, j < (p-1)/2$ so we must have $p \mid i-j$. So there are exactly $(p-1)/2$ quadratic residues mod $p$, leaving $(p-1)/2$ quadratic non-residues.

**Theorem** (Euler): Let $p$ be an odd prime and let $a$ be an integer not divisible by $p$. Then

$$\left(\frac{a}{p}\right) = a^{(p-1)/2} \pmod{p}.$$

*Proof*: If $a$ is a quadratic residue mod $p$ then $a \equiv x^2 \pmod{p}$ where $p \nmid x$ for some $x \in \mathbb{Z}$. Thus

$$a^{(p-1)/2} \equiv (x^2)^{(p-1)/2} \equiv x^{p-1} \equiv 1 \pmod{p}$$

as it should, by Fermat's little theorem. Therefore we have at least $(p-1)/2$ different solutions in $\mathbb{Z}/\langle p\rangle$ to the congruence $X^{(p-1)/2} - 1 \equiv 0 \pmod{p}$. But we know that this polynomial can have at most $(p-1)/2$ solutions, so all the quadratic non-residues do not satisfy this equation. This means that if $a$ is a quadratic non-residue then $a^{(p-1)/2} \not\equiv 1 \pmod{p}$. But $(a^{(p-1)/2})^2 \equiv a^{p-1} \equiv 1 \pmod{p}$ by Fermat's little theorem again, so we must have $a^{(p-1)/2} \equiv -1 \pmod{p}$.

**Corollary**: If $p$ is an odd prime, then the Legendre symbols satisfy:

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

**Corollary**: Let $p$ be an odd prime. Then $-1$ is a quadratic residue mod $p$ if $p \equiv 1 \pmod{4}$ and $-1$ is a quadratic non-residue mod $p$ if $p \equiv 3 \pmod{4}$.

An amazing theorem about Legendre symbols is Gauss's famous law of quadratic reciprocity, which states that if $p$ and $q$ are odd primes then

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}.$$

We'll have more to say about this later.

Now back to that algorithm for finding Fermat's two squares that add up to the prime $p$ if $p \equiv 1 \pmod 4$. It begins with an alternative proof of Lagrange's lemma above. Another way to get a solution to the congruence $x^2 \equiv -1 \pmod p$ is to use Euler's theorem above, as follows: Suppose $a$ is quadratic-non-residue mod $p$, then Euler's theorem tells us that $a^{(p-1)/2} \equiv -1 \pmod p$. But since $p \equiv 1 \pmod 4$, we have $(p-1)/4$ is an integer so we can take $x = [a^{(p-1)/4}]$. Calculating $[a^{(p-1)/4}]$ (by repeated squaring) is much easier than calculating $((p-1)/2)!$ and finding a quadratic non-residue $a$ is easy by trial and error since half the numbers between 1 and $p-1$ work.

Now for the algorithm. Given a prime $p$ such that $p \equiv 1 \pmod 4$, choose a solution to the congruence $x^2 \equiv -1 \pmod p$ such that $0 < x < p/2$ (Why can this always be done?). Then use the Euclidean algorithm on $p$ and $x$. The first two remainders $a$ and $b$ in the process such that both $a$ and $b$ are less than $\sqrt{p}$ will satisfy $a^2 + b^2 = p$. That's it.

Here are a couple of examples:

Suppose $p = 41$. Then $x = 9$ satisfies $x^2 \equiv -1 \pmod{41}$. And the Euclidean algorithm applied to 41 and 9 gives:

| $i$ | $-1$ | $0$ | $1$ | $2$ | $3$ | $4$ |
|---|---|---|---|---|---|---|
| $r_i$ | 41 | 9 | 5 | 4 | 1 | 0 |
| $q_i$ | – | – | 4 | 1 | 1 | 4 |
| $\lambda_i$ | 1 | 0 | 1 | $-1$ | 2 | $-9$ |
| $\mu_i$ | 0 | 1 | $-4$ | 5 | $-9$ | 41 |

The first two remainders less than $\sqrt{41}$ are 5 and 4 and $41 = 5^2 + 4^2$.

Let $p = 113$. Then $x = 15$ satisfies $x^2 \equiv -1 \pmod{113}$. So

| $i$ | $-1$ | $0$ | $1$ | $2$ | $3$ | $4$ |
|---|---|---|---|---|---|---|
| $r_i$ | 113 | 14 | 8 | 7 | 1 | 0 |
| $q_i$ | – | – | 7 | 1 | 1 | 7 |
| $\lambda_i$ | 1 | 0 | 1 | $-1$ | 2 | $-15$ |
| $\mu_i$ | 0 | 1 | $-7$ | 8 | $-15$ | 113 |

We conclude that $113 = 8^2 + 7^2$.

Finally, we do an extension of Euclid's proof on infinitely many primes to primes congruent to 1 mod 4, using Gaussian integers.

**Lemma**: A prime number $p \equiv 3 \pmod 4$ is a prime element in $\mathbb{Z}[i]$.

*Proof.* Suppose $z = a + bi$ is a prime element in $\mathbb{Z}[i]$ that divides $p$, so $p = zy$ for some $y \in \mathbb{Z}[i]$. Since $N(p) = p^2$ we have $N(z) = p$ or $N(z) = p^2$. But $N(z) = c^2 + d^2$ cannot equal $p$ since the sum of two squares cannot be congruent to 3 mod 4, but then $N(y) = 1$ so $y$ is a unit and $p$ was prime in $\mathbb{Z}[i]$.

**Lemma**: If $p$ is an odd prime number dividing $x^2 + 1$ for some $x \in \mathbb{Z}$, then $p \equiv 1 \pmod 4$.

This is because $x^2 + 1 = (x + i)(x - i)$ in $\mathbb{Z}[i]$ and $p$ doesn't divide either factor so can't be prime in $\mathbb{Z}[i]$.

**Theorem**: There are infinitely many primes congruent to 1 mod 4.

If only finitely many, say they are $p_1, \ldots, p_n$, then form the number $M = (p_1 p_2 \cdots p_n)^2 + 1$. Then $M$ is not a power of 2 (why?) so it's divisible by an odd prime, which must be congruent to 1 mod 4, but none of the $p_i$'s divide $M$. So there must be more of them.

This is a really special case of a celebrated result of Dirichlet on primes in arithmetic progressions. We'll prove a less special case later.