Number Theory: summary of notes

Robin Chapman

19 February 2008

Let $\mathbf{N}$ denote the set of positive integers and $\mathbf{Z}$ denote the set of all integers.

Let a and b be integers. We say that a *divides* b (or a is a *divisor* of b, or a is a *factor* of b, or b is a *multiple* of a, or b is *divisible* by a) if there is an integer c with $b = ac$. We write $a \mid b$ to denote that a divides b and $a \nmid b$ if a does not divide b.

A *prime number* or just a *prime* is a number $p \in \mathbf{N}$ such that

- $p > 1$, and
- if $a \in \mathbf{N}$ is a divisor of p then $a = 1$ or $a = p$.

Theorem 1 *Every integer $n \geq 2$ has the form $p_1 \cdots p_k$ where the p_i are prime.*

Proof We use induction. The base case is $n = 2$ which is a prime. In general assume that all numbers from 2 to n have prime factorizations; we claim $n+1$ does too. If $n+1$ is prime, all is well; otherwise $n+1 = ab$ where $a > 1$ and $b > 1$. Thus $a < n+1$ and $b < n+1$ and so a and b have prime factorizations, by the inductive hypothesis. Putting these together gives a prime factorization for $n+1$. By induction each integer $n \geq 2$ has a prime factorization. $\square$

Theorem 2 (Euclid) *There are infinitely many primes.*

Proof It suffices to prove that for each $n \in N$, there is a prime $p > n$. Let $N = n! + 1$. Then N has a prime factorization, so it has a prime factor p. We claim that $p > n$. Otherwise $p \leq n$ and so p must divide $n!$, but p cannot divide both the consecutive numbers $n!$ and $n! + 1$ — contradiction. Hence we must have $p > n$. $\square$

For a, $b \in \mathbf{Z}$ and $n \in N$ we say that *a is congruent to b modulo n* if $n \mid (a-b)$. We write $a \equiv b \pmod{n}$ when a is congruent to b modulo n. Congruences respect the operations of addition, subtraction and multiplication, but not division.

Given n, each integer is congruent to exactly one of the numbers 0, 1, $2, \ldots, n-1$ modulo n. Similarly each integer is congruent to exactly one number a with $-n/2 < a \leq n/2$ modulo n.

Theorem 3 *There are infinitely many primes p such that $p \equiv 3 \pmod{4}$.*

Proof It suffices to prove that for each $n \in \mathbf{N}$, there is a prime $p > n$ with $p \equiv 3 \pmod{4}$. Let $N = 4(n!) - 1$. Then N has a prime factorization: $N = p_1 p_2 \cdots p_n$. We claim that one of the p_i satisfies $p_i \equiv 3 \pmod{4}$. As N is odd, none of the p_i have $p_i \equiv 0$ or $p_i \equiv 2 \pmod{4}$ so they all have have $p_i \equiv 1$ or $p_i \equiv 3 \pmod{4}$. But they can't **all** have $p_i \equiv 1 \pmod{4}$ since then $N \equiv 1 \times 1 \times \cdots \times 1 = 1 \pmod{4}$ but $N = 4(n!) - 1 \equiv -1 \equiv 3 \pmod{4}$. So at least one of the p_i satisfies $p_i \equiv 3 \pmod{4}$. Let's write this p_i as p.

We claim that $p > n$. Otherwise $p \leq n$ and so p must divide $n!$ and so also $4(n!)$, but p cannot divide both the consecutive numbers $4(n!) - 1$ and $4(n!)$ — contradiction. Hence we must have $p > n$. $\square$

The Euclidean algorithm takes a, $b \in \mathbf{N}$ and finds their greatest common divisor. More precisely it finds r, $s \in \mathbf{Z}$ such that $g = ra + sb$ is a divisor of both a and b; any common divisor of a and b must also divide $ra + sb = g$ so then g is the largest possible common divisor of a and b. We write $\gcd(a, b)$ for the greatest common divisor of a and b. We say that a and b are *coprime* if $\gcd(a, b) = 1$.

To perform the Euclidean algorithm we may assume that $a \geq b$. Define $a_1 = a$ and $a_2 = b$. We produce a sequence $a_1, a_2, \ldots, a_k$ of positive integers ending when $a_k \mid a_{k-1}$. If at some stage we have reached a_j but $a_j \nmid a_{j-1}$ we define a_{j+1} by $a_{j+1} = a_{j-1} - q_j a_j$, where $0 < a_{j+1} < a_j$, that is the remainder when a_{j-1} is divided by a_j. As $a_2 > a_3 > a_4 > \cdots > 0$ the sequence must terminate. Set $g = a_k$ if the sequence terminates at a_k. Then $g \mid a_{k-1}$ and $g \mid a_k$ obviously. It follows that $g \mid a_{k-2}$, $g \mid a_{k-3}$ and so on. Eventually we get $g \mid a_2$ and $g \mid a_1$. Thus g is a common factor of a and b.

TO find integers r and s such that $g = ra + sb$ we keep track at each stage of r_j and s_j such that $a_j = r_j a + s_j b$. We start with $r_1 = 1$, $s_1 = 0$, $r_2 = 0$ and $s_2 = 1$. Then define recursively $r_{j+1} = r_{j-1} - q_j r_j$ and $s_{j+1} = s_{j-1} - q_j s_j$. Then it's easy to check that $a_j = r_j a + s_j b$ for all j. Set $r = r_k$ and $s = s_k$. Then $g = ra + sb$. If h is a common factor of a and b it divides ra and sb and so also $g = ra + sb$. Thus g really is the greatest common divisor of a and b.

Consider a congruence

$$ax \equiv b \pmod{n}. \tag{$*$}$$

When $\gcd(a, n) = 1$ this congruence has a unique solution modulo n. To see this, by the Euclidean algorithm, there are r and s with $1 = \gcd(a, n) = ra + sn$. Thus $ra \equiv 1 \pmod{n}$ and so

$$x = 1x \equiv rax \equiv rb \pmod{n}$$

and this really is a solution as

$$a(rb) = (ra)b \equiv 1b = b \pmod{n}.$$

In particular for prime p consider the congruence

$$ax \equiv 1 \pmod{p}. \tag{$\dagger$}$$

As $\gcd(a, p) = 1$ unless $p \mid a$ then when $p \nmid a$ there is a unique solution to (†). Call a solution a *reciprocal* of a modulo p.

Theorem 4 (Euclid's lemma) *If $p \mid ab$ with p prime then either $p \mid a$ or $p \mid b$.*

Proof If $p \nmid a$ then a has a reciprocal c modulo p: $ca \equiv 1 \pmod{p}$. Thus

$$b = 1b \equiv cab \equiv c0 = 0 \pmod{p},$$

that is $p \mid b$. □

One can extend this: if $p \mid a_1 a_2 \cdots a_n$ then p divides at least one of the a_i.

Theorem 5 *If $a^2 \equiv 1 \pmod{p}$ with p prime, then $a \equiv \pm 1 \pmod{p}$.*

Proof If $a^2 \equiv 1 \pmod{p}$ then $p \mid (a^2 - 1)$, that is $p \mid (a - 1)(a + 1)$. By Euclid's lemma, either $p \mid (a - 1)$ or $a \mid (a + 1)$, that is either $a \equiv 1 \pmod{p}$ or $a \equiv -1 \pmod{p}$. □

Theorem 6 (Wilson) *If p is prime then $(p - 1)! \equiv -1 \pmod{p}$.*

Proof Pair up the numbers $1, 2, \ldots, p-1$ with their reciprocals modulo p. By the previous theorem only the numbers 1 and $p - 1$ are paired with themselves. The numbers $2, 3, \ldots, p-2$ fall into pairs whose products are 1 modulo p. Hence

$$(p - 2)! = 2 \times 3 \times \cdots \times (p - 2) \equiv 1 \pmod{p}.$$

Multiplying by $p - 1$ gives

$$(p - 1)! \equiv p - 1 \equiv -1 \pmod{p}.$$

□

Theorem 7 (Unique factorization) *If $p_1 \cdots p_j = q_1 \cdots q_k$ where each p_i and q_i is prime, and $p_1 \le p_2 \le \cdots \le p_j$ and $q_1 \le q_2 \le \cdots \le q_k$ then $j = k$ and $p_i = q_i$ for each i.*

Proof If $p_1 = q_1$ then $p_2 \cdots p_j = q_2 \cdots q_k$ are two prime factorizations of a smaller number, and an appeal to strong induction settles the result. Hence we only need show that $p_1 = q_1$ and we do that by assuming $p_1 \ne q_1$ and deriving a contradiction.

Suppose that $p_1 \ne q_1$. Either $p_1 < q_1$ or $p_1 > q_1$. Well consider only the case where $p_1 < q_1$ as the other can be done by swapping the rôles of the ps and qs. As $p_1 \mid (p_1 \cdots p_j)$ then $p_1 \mid (q_1 \cdots q_k)$. By the comment after Euclid's lemma, $p_1 \mid q_i$ for some i. But $p_1 < q_1 \le q_i$ and q_i is prime. So q_i cannot have the factor p_1 as $1 < p_1 < q_i$. This is a contradiction. □

Theorem 8 (Fermat's little theorem) *Let p be prime, and $p \nmid a$. Then $a^{p-1} \equiv 1 \pmod{p}$.*

Proof Consider the list of numbers a, $2a$, $3a, \ldots, (p-1)a$. For $1 \le k \le p-1$ the congruence $ax \equiv j \pmod{p}$ has a unique solution modulo p. Thus a, $2a$, $3a, \ldots, (p-1)a$ are congruent modulo p to $1, 2, 3, \ldots, p-1$ in some order. Taking the product gives

$$a(2a)(3a)\cdots((p-1)a) \equiv 1 \times 2 \times 3 \times \cdots \times (p-1) \pmod{p}$$

that is

$$(p-1)!a^{p-1} \equiv (p-1)! \pmod{p}.$$

By Wilson's theorem

$$-a^{p-1} \equiv -1 \pmod{p}.$$

Now negate! □

Theorem 9 *Let p be prime. The congruence $x^2 \equiv -1 \pmod{p}$ is soluble if and only if $p = 2$ or $p \equiv 1 \pmod{4}$.*

Proof If $p = 2$ then $x = 1$ is a solution. Then we may suppose p odd so that $p \equiv 1$ or $3 \pmod{4}$.

The easier case is $p \equiv 3 \pmod{4}$. Write $p = 4k + 3$. If $x^2 \equiv -1 \pmod{p}$ then

$$x^{4k+2} = (x^2)^{2k+1} \equiv (-1)^{2k+1} = -1 \pmod{p}.$$

But $4k + 2 = p - 1$ and by Fermat's little theorem, $x^{p-1} \equiv 1 \pmod{p}$. This is a contradiction. So $x^2 \equiv -1 \pmod{p}$ is insoluble.

The other case is $p \equiv 1 \pmod 4$. Write $p = 4k + 1$. We claim that $x = (2k)!$ is a solution. By Wilson's theorem

$$\begin{aligned}
-1 &\equiv (p-1)! = (4k)! \\
&= 1 \times 2 \times 3 \times \cdots \times (2k) \times (2k+1) \times (2k+2) \times \cdots \times (4k) \\
&= 1 \times 2 \times 3 \times \cdots \times (2k) \times (p-2k) \times (p-2k+1) \times \cdots \times (p-1) \\
&\equiv 1 \times 2 \times 3 \times \cdots \times (2k) \times (-2k) \times (-(2k-1)) \times \cdots \times (-1) \\
&= (-1)^{2k} 1 \times 2 \times 3 \times \cdots \times (2k) \times (2k) \times (2k-1) \times \cdots \times 1 \\
&= (2k)!^2 \pmod p.
\end{aligned}$$

□

Given a prime number $p \equiv 1 \pmod 4$ although the theorem gives a formula for a solution of $x^2 \equiv -1 \pmod p$, this formula is completely impractical save for very small p since it requires almost $p/2$ muliplications modulo p. Here is a more practical approach. Set $p = 4k + 1$. Pick a number a at random between 1 and $p - 1$ and compute $b \equiv a^k \pmod p$ (using the repeated squaring trick). Then $b^4 \equiv a^{4k} = a^{p-1} \equiv 1 \pmod p$. Thus $b^2 \equiv \pm 1 \pmod p$. If $b^2 \equiv -1 \pmod p$ we have won! Otherwise start again with a new a. It can be proved (although I won't here) that we win with probability $\frac{1}{2}$, so on average we expect to need two tries.

Theorem 10 *There are infinitely many primes p such that $p \equiv 1 \pmod 4$.*

Proof It suffices to prove that for each $n \in \mathbf{N}$, there is a prime $p > n$ with $p \equiv 1 \pmod 4$. Let $N = 4(n!)^2 + 1$. Then N has a prime factorization and so a prime factor p. As N is odd p is odd. Also $(2(n!))^2 \equiv -1 \pmod p$. By the previous theorem $p \equiv 1 \pmod 4$.

We claim that $p > n$. Otherwise $p \leq n$ and so p must divide $n!$ and so also $4(n!)^2$, but p cannot divide both the consecutive numbers $4(n!)^2$ and $4(n!)^2 + 1$ — contradiction. Hence we must have $p > n$. □

Define $S_2 = \{a^2 + b^2 : a, b \in \mathbf{Z}\}$, the set of sums of two squares of integers.

A Gaussian integer is a complex number of the form $\alpha = a + bi$ where a, $b \in \mathbf{Z}$. It's easy to see that if α and β are Gaussian integers then so are $\alpha + \beta$, $\alpha - \beta$ and $\alpha\beta$. If $\alpha = a + bi$ is a Gaussian integer, then $|\alpha|^2 = a^2 + b^2 \in S_2$. Thus S_2 is the set of all $|\alpha|^2$ as α ranges over the Gaussian integers. This is a very handy observation!

Theorem 11 *If m, $n \in S_2$ then $mn \in S_2$.*

Proof If m, $n \in S_2$ then $m = |\alpha|^2$ and $n = |\beta|^2$ for some Gaussian integers α and β. Then $\alpha\beta$ is a Gaussian integer and

$$mn = |\alpha|^2|\beta|^2 = |\alpha\beta|^2 \in S_2.$$

□

Theorem 12 *If p is prime and $p \equiv 3 \pmod 4$ then $p \mid (a^2+b^2)$ implies that $p \mid a$ and $p \mid b$.*

Proof Let $p \equiv 3 \pmod 4$ and suppose $p \mid (a^2+b^2)$, that is $b^2 \equiv -a^2 \pmod p$. If $p \nmid a$ then there is $c \in \mathbf{Z}$ with $ca \equiv 1 \pmod p$. Then $(cb)^2 \equiv -(ca)^2 \equiv -1 \pmod p$ which is impossible as the congruence $x^2 \equiv -1 \pmod p$ is insoluble. This contradiction proves that $p \mid a$. Similarly $p \mid b$. □

Theorem 13 *If $p \equiv 1 \pmod 4$ then $p \in S_2$.*

Proof There is $c \in \mathbf{Z}$ with $c^2 \equiv -1 \pmod p$. Let

$$A = \{(a, b) : a, b \in \mathbf{Z}, 0 \le a, b < \sqrt{p}\}.$$

Then A is a set of integer points in the plane. As $\sqrt{p}$ is not an integer, then there is an integer k with $k < \sqrt{p} < k + 1$. Then $(a, b) \in A$ if and only if a and b are integers between 0 and k inclusive. Thus A contains $(k + 1)^2$ points. As $(k + 1)^2 > p$, by the pigeonhole principle there are **distinct** points (a_1, b_1), $(a_2, b_2) \in A$ such that $a_1 + cb_1 \equiv a_2 + cb_2 \pmod p$. Let $a = a_1 - a_2$ and $b = b_2 - b_1$. Then $(a, b) \ne (0, 0)$ and $a \equiv cb \pmod p$. Thus $a^2 + b^2 \equiv c^2b^2 + b^2 \equiv 0 \pmod p$. Thus $a^2 + b^2 = mp$ where m is a positive integer. All we need now to prove is that $m = 1$.

As $0 \le a_1 < \sqrt{p}$ and $0 \le a_2 < \sqrt{p}$ then $-\sqrt{p} < a = a_1 - a_2 < \sqrt{p}$ and so $a^2 < p$. Similarly $b^2 < p$. Hence $mp = a^2 + b^2 < 2p$ and we conclude that $m = 1$. □

Theorem 14 *Let $n = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$ with $p_1 < p_2 < \cdots < p_k$ prime then $n \in S_2$ if and only if r_i is even for every i with $p_i \equiv 3 \pmod 4$.*

Proof Suppose that $n \in S_2$ and that $p = p_i \equiv 3 \pmod 4$. We need to prove that $r = r_i$ is even. Note that $n = p^r m$ where $p \nmid m$. We argue by induction on r that r is] even. If $r = 0$ there is nothing to prove. If $r > 0$, write $p = a^2 + b^2$ with a, $b \in \mathbf{Z}$. By Theorem 12 $p \mid a$ and $p \mid b$. Thus $p^{r-2}m = c^2 + d^2$ where $c = a/p \in \mathbf{Z}$ and $d = b/p \in \mathbf{Z}$. By the inductive hypothesis $r-2$ is even. Hence r is even. Thus the given condition on n is necessary for n to lie in S_2.

Conversely suppose that $n = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$ with the p_i prime and with r_i is even whenever $p_i \equiv 3 \pmod 4$. Then n is a product of squares p_i^2 and primes p_i with $p_i = 2$ or $p_i \equiv 1 \pmod 4$. Of course $2 = 1^2 + 1^2 \in S_2$ and as all these factors lie in S_2 so does n as S_2 is closed under multiplication. $\square$