

MATHEMATICS 350 FALL 2008 (SHATZ)
Assignment II, September 22, 2008. Due October 6, 2008

The following is from Dante's Comedy, Canto 26, Inferno (The Canto of Ulysses):

“Considerate la vostra semenza:
fatti non foste a viver come bruti
ma per seguir virtute e conoscenza.”

More Ulysses, this time by Tennyson:

“... Come my friends,
'Tis not too late to seek a newer world.
Push off, and sitting well in order to smite
The sounding furrows; for my purpose holds
To sail beyond the sunset, and the baths
Of all the Western stars, until I die.
It may be that the gulfs will wash us down:
It may be we shall touch the Happy Isles,
And see the great Achilles, whom we know.
Tho' much is taken, much abides; and tho'
We are not now that strength which in old days
Moved earth and heaven; that which we are, we are;
One equal temper of heroic hearts,
Made weak by time and fate, but strong in will
To strive, to seek, to find, and not to yield.”

A PROBLEMS (NOT TO BE HANDED IN).

AI Show that for each pair of positive integers, n and q , the number $\frac{(qn)!}{(n!)^q}$ is an integer. Suggestion: Our number counts something—hence is an integer, describe what it counts and prove that it counts these.

AII (Perfect medians again.) Consider the sequence $1, 3, 5, \dots, n$ for n an odd integer. For which such n does our sequence possess a perfect median? Are there infinitely many n for which a perfect median exists; can you give an algorithm to find them all?

AIII Suppose that Euler's guess that the size of the n^{th} prime number, p_n , satisfies

$$p_n \sim n \log(n)$$

is correct. Find a simple function $f(x)$ (such as you would have understood in the first week of any beginning calculus class) so that, if we write $\pi(x)$ for the number of primes $\leq x$, we have

$$\pi(x) \sim f(x) \quad x \rightarrow \infty.$$

Show also that

$$\pi(x) \sim \int_2^x \frac{dx}{\log(x)}.$$

It turns out that the latter integral is a better estimate for $\pi(x)$ than the simple $f(x)$ you made.

B PROBLEMS (TO BE HANDED IN–GROUP WORK).

BI a) A certain farmer possesses a great bunch of corn ears which he wishes to sell. He tries packaging them in bunches of 2 and finds one is left over. He tries bunches of 3 ears and again there is one left over, and so on for each of the tried packages of 4, 5, 6 ears at a time—each yields one extra corn ear left over. Then, when he tries bunches of 7 ears at a time, they fit into equal packages and none are left over. The obvious question is: How many ears of corn did he start with? But there are many solutions to this question. If we label the *solutions* by increasing numbers of ears of corn, say S_1, S_2, \dots, S_n , find S_5 . Can there be an infinite number of solutions; that is, is there always an S_n for every n ?

b) Now, for each j , let a_j be an integer with $0 \leq a_j < j$ and take j to be 2, 3, 4, 5, 6, 7. Does there always exist an integer n so that n divided by j leaves the remainder a_j ? (Remember, n is fixed and must work for all the j with $j = 2, 3, 4, 5, 6, 7$.) If you decide the answer is “yes”, give a proof and find all such n that work. If you decide the answer is “no”, give a condition on the numbers a_j which will guarantee the existence of a solution, prove that this does indeed guarantee existence of a solution and find all solutions to the problem with your given a_j .

BII a) We suppose given on the set of integers, \mathbf{Z} , a non-negative real valued function $V(n)$ which satisfies the rules:

$$i) V(n+m) \geq \min\{V(n), V(m)\},$$

$$V(n+m) = \min\{V(n), V(m)\} \text{ if } V(n) \neq V(m)$$

$$ii) V(nm) = V(n) + V(m)$$

$$iii) V(0) = \infty. \text{ Here, } \infty > \alpha \text{ and } \infty \pm \alpha = \infty, \text{ where } \alpha \text{ is any real number.}$$

As an example of such a function (not identically zero except for its value of ∞ on zero), we fix a prime number, p , and we define the function ord_p by: $ord_p(n)$ is the maximum integer r so that p^r divides n . Then you check easily that ord_p is a function V as described above. Show that *every* function

V , satisfying our rules, (not identically zero) has the form $Kord_p$ for some real constant K and for a unique prime number p (which depends on V).

b) If p is a prime number, let us write $\|n\|_p$ for the function given by $(\frac{1}{p})^{ord_p(n)}$. Then the function $\|n\|_p$ satisfies rules analogous to *i*), *ii*), *iii*) above—you should write down these rules in the new form. Consider a function ϕ satisfying the analogs of *ii*), *iii*) and the rule

$$\phi(n+m) \leq C \max\{\phi(n), \phi(m)\}$$

where C is a real constant ≥ 1 (instead of the strict analog of *i*) in which $C = 1$). Notice that any real positive power of such a function, namely ϕ^α , again satisfies all the rules for ϕ ; so, if we consider powers of such functions as essentially the same as the functions themselves (just as multiples of ord_p were admitted as “the same as” ord_p), we may and *henceforth do* assume that our constant C satisfies $C \leq 2$. Show that

$$\phi(a+b) \leq \phi(a) + \phi(b).$$

(I suggest you first show that

$$\phi(a_1 + a_2 + \cdots + a_n) \leq 2n \max\{\phi(a_1), \cdots, \phi(a_n)\}.$$

Then, consider $\phi(a+b)^n$ and finally take n^{th} roots.)

c) It proves convenient to extend the definition of our ϕ to encompass its values on rational numbers. We do this by the simple expedient of setting $\phi(\frac{a}{b}) = \frac{\phi(a)}{\phi(b)}$. Notice that there are only two types of ϕ : Those with $C = 1$ and those with $C > 1$; here, we always pick the smallest C that can be used for a given ϕ . The first type come from functions V as in part a) (simply take $\log(\phi)$ as V); we are now concerned with the second type. For these, I remind you, we take $C \leq 2$. Pick two integers m, n both > 1 and show that given t , we can write

$$m^t = a_0 + a_1 n + a_2 n^2 + \cdots + a_s n^s$$

for some s and some choice of a_j , with $0 \leq a_j < n$ and $a_s \neq 0$. Use this to show that

$$s \leq t \left(\frac{\log(m)}{\log(n)} \right),$$

and

$$\phi(m^t) \leq n \left(1 + t \left(\frac{\log(m)}{\log(n)} \right) \right) (\max\{1, \phi(n)\})^{t \left(\frac{\log(m)}{\log(n)} \right)}.$$

From this, deduce that

$$\phi(m) \leq (\max\{1, \phi(n)\})^{\frac{\log(m)}{\log(n)}}.$$

Now $C > 1$ so for every $n > 1$ we have $\phi(n) > 1$ (WHY?). So, we can rewrite the above as

$$\phi(m)^{\frac{1}{\log(m)}} \leq \phi(n)^{\frac{1}{\log(n)}},$$

and this holds for all $m, n > 1$. Finally, deduce that $(\exists \alpha)(\phi(n) = |n|^\alpha)$. What you will have proved is that (up to “essentially the same”) there are two kinds of ϕ : The $\|n\|_p$ and $|n|$ —denote this latter by the symbol $\|n\|_\infty$.

d) Write P for the set whose elements are the various prime numbers, p , and the extra element ∞ . For each rational number, r , prove that

$$\prod_{w \in P} \|r\|_w = 1.$$

BIII The French jurist Pierre de Fermat (1601-1665) was also an amateur mathematician, perhaps the greatest amateur ever in mathematics. He corresponded with all the savants of his day, made contributions to (what later became) differential calculus, to physics, geometry, and above all to number theory. In the latter subject, he was stimulated by reading Bachet’s Latin Translation of Diophantos’ (fl. first century AD) book: *Αρηθμετικα*. In his copy of this work, he made annotations, stated new results (but rarely gave any proofs), and introduced new methods. At his death, his son collected these varia and published them and by the end of the eighteenth century all but one of his statements (proofs omitted by him) had received proofs by the mathematicians of the day. The one remaining statement (see below for his Latin version of it) was dubbed “Fermat’s Last Theorem” and it states in symbols that the equation $x^n + y^n = z^n$ has no solution in integers x, y, z with $xyz \neq 0$ provided $n \geq 3$. We can write FLT(n) for the statement that FLT is true for that fixed n . Here is what Fermat said in the margin of his copy of Diophantos:

“Cubum autem in duos cubos, aut quadrato-quadratum in duos quadrato-quadratos, et generaliter, nullem in infinitum ultra quadratum potestatum in duos ejusdem nominis fas est dividere; cujus rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet.”

The history of attempts at proofs of the FLT is rich and, for various low (and not so low) values of n , FLT(n) was proved. But, n is allowed to be anything above 2 and there are infinitely many such n . Finally, using methods not by any stretch of imagination available to Fermat, Andrew Wiles proved FLT(n) for all $n \geq 3$ in 1994. However, in the last 20 years of the last century, mathematicians saw that an interesting statement connecting addition and prime factorization might be true (it is NOT yet proved) and that this statement gave a proof of FLT as a corollary. Your task in this problem is to take this statement (called the ABC conjecture) and provide from it a proof of Fermat’s Last Theorem.

To state the ABC conjecture, we need a bit of notation: If m is an integer,

we know we can factor it into a product of prime powers, say $m = \prod_j p_j^{r_j}$. Here, the r_j may very well be integers > 1 (since we assume when we write the product that the various p_j are distinct for distinct j). Define $G(m)$ to be $\prod_j p_j$. Notice that the difference between m and $G(m)$ is that all the r_j have been put equal to 1 in the expression for $G(m)$. Now we can state the ABC conjecture.

The ABC Conjecture of Masser and Osterlé:

If A, B, C are relatively prime integers and $A + B + C = 0$ then

$$(\forall \epsilon > 0)(\exists K(\epsilon))(\max\{|A|, |B|, |C|\} \leq K(\epsilon)G(ABC)^{1+\epsilon}),$$

where $K(\epsilon)$ is a positive real constant that depends on ϵ but is *independent* of A, B, C .

Use the ABC conjecture to prove that $(\exists N)(n > N \implies FLT(n))$. In fact, if you pick ϵ and know $K(\epsilon)$, give an estimate for how large N has to be in terms of $K(\epsilon)$. Since N is explicitly bounded the remaining cases of $FLT(n)$, for $n \leq N$, form a finite number of cases of the FLT, therefore FLT is essentially proved (from ABC).