

Math 216
Practice Problems A

A1. (Bernoulli's inequality) For any real number $x > -1$, and integer $n > 1$, prove by induction that $(1 + x)^n > 1 + nx$. If $x \geq 0$, this can be proved easily, without induction. How?

A2. Use the formula you derived in problem 2.2b to prove by induction that

$$\int_0^{\pi/2} \sin^{2k+1} x \, dx = \frac{2 \cdot 4 \cdots (2k)}{1 \cdot 3 \cdots (2k+1)}.$$

A3. Find the orders of all the elements of \mathbb{Z}_{11}^\times and \mathbb{Z}_{17}^\times .

A4. Prove that there are infinitely many primes of the form $8k+1$. (Use the method of Fermat numbers, plus the Proposition from class Feb 8.)

A5. Prove that there are infinitely many primes of the form $4096k+1$ (Same method as above, note $4096 = 2^{12}$.) As recreation, you might try to find a single such prime.

A6. Prove, with your bare hands (and maybe a pencil, though even that is not necessary) that the number $2^{100} - 1$ is divisible by 101. It does not help to know that $2^{100} - 1 = 1267650600228229401496703205375$.

A7. Use the factorization in problem 2.2 to prove that if $a^m - 1$ is prime and $m > 1$ then $a = 2$ and m is prime. (Hint for the second part: if $m = kl$ then $a^m = (a^k)^\ell$.)

A8. Use A6 to find more prime divisors of $2^{100} - 1$.

A9. Use the factorization in problem 2.3 to prove that if $a^m + 1$ is prime then $m = 2^d$ for some n . (Hint for the second part: If $m = (2k+1)2^d$, then $a^m = (a^{2^d})^{(2k+1)}$.)

A10. The number 19457 is prime. I don't know if $2^{19457} - 1$ is prime. What does the third Book proof (top of page 4) tell us about the prime factors of $2^{19457} - 1$?

A11. Write down the definitions of: Group, Subgroup, Equivalence Relation. Then prove that if G is a group, and H is a subgroup of G then the relation $a \sim b$ if $a = bh$ for some $h \in H$ is an equivalence relation on G . (We used this fact in the proof of Lagrange's theorem.)

A12. Suppose $p > 2$. In problem 3.4 you proved that the product $[1][2] \cdots [p-1]$ of all the elements in \mathbb{Z}_p^\times is $[p-1]$, which is the same as $[-1]$. Rewrite this product to show that

$$([1][2] \cdots [\frac{p-1}{2}])^2 = [-1]^{(p+1)/2}.$$

Hint: $[\frac{1+p}{2}] = [\frac{1-p}{2}]$, $[\frac{3+p}{2}] = [\frac{3-p}{2}]$, ...

A13. Using Lagrange's theorem, we have seen that if -1 is a square mod p then $p = 4k+1$. Use A12 to prove the converse, namely that if $p = 4k+1$, then -1 is a square mod p . Also give an explicit formula for the square root of -1 mod p .

A14. Memorize the first three Book proofs of the infinitude of primes. Summarize all the modifications (that we have learned so far) which prove that other congruence classes contain infinitely many primes.