MAT 311: Number Theory
Spring 2006

HW2 - Solutions

1. (Davenport, pp.215-216, ex. 1.04) In general, given any positive integer n, then $\{(n+1)! + m : 2 \leq m \leq n+1\}$ is a set of n consecutive composite numbers, because m divides $(n+1)!$ (and hence $(n+1)! + m$) whenever $2 \leq m \leq n+1$.

2. (Davenport, pp.215-216, ex.1.05) If we evaluate $n^2 + n + 41$ for first few $n = 0, 1, 2, \ldots$ we see that they turn out to be primes. However, for $n = 40$, we have $n^2 + n + 1 = 41^2$ which is composite. Alternatively, $n = 41$ actually divides $n^2 + n + 41$ since each term is divisible by 41. It is an interesting fact that for $n = 0, 1, \ldots, 39$ this expression gives prime numbers. This can be checked easily by writing a simple program (for instance in `pari`)

   ```
   for(n=0,40, if(isprime(n)=0, print(n)))
   ```

   which will print 40 as output.

3. (Davenport, pp.215-216, ex. 1.11) Assume that n is a composite number, say $n = ab$, where $a, b \geq 2$. We want to show that $2^n - 1$ cannot be prime. Indeed,

   $$2^n - 1 = 2^{ab} - 1 = (2^a)^b - 1 = (2^a - 1)((2^a)^{b-1} + (2^a)^{b-2} + \cdots + (2^a)^1 + 1).$$

   Now, since $a \geq 2$, we have $2^a - 1 \geq 3$. Moreover, $2^a - 1$ is strictly less than $2^n - 1$ since $a < n$. Hence $2^n - 1$ is a product of two numbers both of which are > 1. Therefore, $2^n - 1$ cannot be a prime. The converse does not hold, as for $n = 11$, we have $2^{11} - 1 = 23 \cdot 89$.

4. (Davenport, pp.215-216, ex. 1.12) Assume that n is not a power of 2. Then there is an *odd* integer m dividing n, so we can write $n = mk$ for some $k > 1$. Then we have

   $$2^n + 1 = (2^k)^m + 1 = (2^k + 1)((2^k)^{m-1} - (2^k)^{m-2} + \cdots - (2^k)^1 + 1).$$

   Similarly, $2^k + 1$ is a number greater than 1 but strictly less than $2^n + 1$ which divides $2^n + 1$. Hence $2^n + 1$ cannot be a prime. The converse does not hold here either: $2^{(2^5)} + 1$ is divisible by the prime 641.

5. Let $\operatorname{sq}(x)$ denote the number of squares less than x. We claim that $\operatorname{sq}(x) =$ the greatest integer less than $\sqrt{x}$, denoted by $\lfloor\sqrt{x}\rfloor$. Given $x \in \mathbb{R}$. Let $S = \{1^2, 2^2, \ldots, m^2\}$ be the set of squares less than x (listed in increasing order). Then clearly $\operatorname{sq}(x) = m$, that is, $\operatorname{sq}(x)$ is equal to the largest

integer m whose square is less than x. We claim that $m = \lfloor\sqrt{x}\rfloor$. Indeed, since $\lfloor\sqrt{x}\rfloor < \sqrt{x}$, we have $\lfloor\sqrt{x}\rfloor^2 < x$. So $\lfloor\sqrt{x}\rfloor$ is an integer whose square is less than x. This shows $\lfloor\sqrt{x}\rfloor \leq \mathrm{sq}(x) = m$. Conversely, if k is an integer that is strictly grater that $\lfloor\sqrt{x}\rfloor$, then $k^2 \geq (\lfloor\sqrt{x}\rfloor + 1)^2 > (\sqrt{x})^2 = x$. Therefore, $m = \mathrm{sq}(x) \leq \lfloor\sqrt{x}\rfloor$. Combining it with the previous reverse inequality we obtain that $\mathrm{sq}(x) = \lfloor\sqrt{x}\rfloor$, as required.

To show why *most numbers are non-square*, we need to consider the limit of the ratio (number of all squares $< x$)/ (all numbers $< x$) as $x \to \infty$. Indeed, this limit can be computed as

$$\lim_{x\to\infty} \frac{\mathrm{sq}(x)}{\lfloor x\rfloor} = \lim_{x\to\infty} \frac{\lfloor\sqrt{x}\rfloor}{\lfloor x\rfloor} \leq \lim_{x\to\infty} \frac{\sqrt{x}}{x-1} = 0$$

So the limit we were looking for is 0. That means, as x gets larger, the number of squares less than x is 'negligible' compared to x.

6. We would like to show that there are no prime triplets $(p, p+2, p+4)$ other than $(3, 5, 7)$. To show this note that among any n consecutive numbers there is one divisible by n. In particular, one of $p, p+1, p+2$ is divisible by 3. Thus, one of $p, p+2, p+4$ is divisible by 3 (note that $3|p+1$ iff $3|p+4$). Hence, if $(p, p+2, p+4)$ is a *prime* triplet, this forces p to be actually equal to 3 (if not, then $p, p+2, p+4$ are all primes > 3 and divisible by 3, a contradiction). So we conclude that $(3, 5, 7)$ is the only prime triplet.

7. We will show that every integer > 11 is the sum of two composite integers. Indeed, if n is even, then $n = (n-4)+4$; and if it is odd, then $n = (n-9)+9$ is a sum of two composite numbers. In the first case, $n-4$ is an even number strictly greater than 7 (hence necessarily composite); and in the latter case $n-9$ is an even number strictly greater than 2 (hence again composite).

8. We will show that there are no primes of the form N^3+1 for $N > 1$. Indeed, we can factorize the expression as $N^3+1 = (N+1)(N^2-N+1)$. The first factor is > 2 and strictly smaller than N^3+1. Hence N^3+1 cannot be prime.

9. The smallest five consecutive composite numbers are $24, \ldots, 28$.