Math 255 - Spring 2018
Homework 6 Solutions

1. We first let $m = 1$. In that case, Lemma 6 says that if $p|a_1$, then $p|a_i$ for $1 \leq i \leq 1$, or in other words that $p|a_1$. This is exactly what we assume so it is true.

   (It turns out that there is no need to do $m = 2$ separately since the induction step will take care of it. Therefore we don't.)

   Now let $k \geq 2$, and assume by induction that Lemma 6 is true for $m = k - 1$. In other words, assume that if $a_1, \ldots a_{k-1}$ are integers and p divides the product $a_1 \cdots a_{k-1}$, then $p|a_i$ for some $1 \leq i \leq k - 1$.

   Now consider k integers $a_1, \ldots a_k$, and assume that p divides the product $a_1 \cdots a_k$. By associativity, we can write this product as

$$a_1 \cdots a_k = (a_1 \cdots a_{k-1}) \cdot a_k,$$

   and $a_1 \cdots a_{k-1}$ is itself one integer. Since p is prime and p divides the product of $a_1 \cdots a_{k-1}$ and a_k, p must either divide $a_1 \cdots a_{k-1}$ or p divides a_k. If p divides a_k, we are done, because in that case $p|a_i$ for $i = k$.

   If p divides $a_1 \cdots a_{k-1}$, then by induction p divides a_i for some $1 \leq i \leq k - 1$. In that case we are done as well, and the lemma is proved by induction.

2. Since $n > 1$ in this Lemma, the base case is $n = 2$. We know that 2 is prime, and therefore it is a product of primes (only one prime, but that still counts).

   We now fix k, and assume by (strong) induction that Lemma 2 is true for all integers $2, 3, \ldots, k - 1$. In other words the integers $2, 3, \ldots, k - 1$ are all products of primes.

   Consider now $n = k$. We know by Lemma 1 that k is divisible by a prime. Write $k = p\ell$, where p is prime and ℓ is an integer. Since $p > 1$ (because it is prime), it follows that $1 \leq \ell < k$. If $\ell = 1$, we are done because k is prime and therefore a product of primes.

   If $1 < \ell < k$, then by strong induction ℓ is a product of primes, say $\ell = p_1 p_2 \cdots p_r$ for some r. Then $k = p p_1 p_2 \cdots p_r$ is also a product of primes, and the lemma is proved by induction.

3. (a) Since $\sqrt{200} \approx 14.14$, it suffices to check all of the multiples of all of the primes less than or equal to $N = 15$ (we must round up to be safe, since $14^2 = 196$). In other words, once we have crossed out the multiples of 13, all remaining integers on the grid will be prime.

   (b) For this problem please see the grid on the last page of these solutions.

4. If $p > n^{1/3}$, then $\frac{1}{p} < \frac{1}{n^{1/3}}$, from which it follows that $\frac{n}{p} < \frac{n}{n^{1/3}} = n^{2/3}$.

   For simplicity, write $d = \frac{n}{p}$; this is an integer since p divides n. Suppose further by way of contradiction that d is not prime. In that case, by Lemma 4, d has a prime divisor, let's call it q, that is less than or equal to $d^{1/2}$. Since we have $d < n^{2/3}$, it follows that $q < (n^{2/3})^{1/2} = n^{1/3}$.

We now note that since q divides d and d divides n, by Exercise 2 of Section 1, q divides n. Therefore q is a prime factor of n that is strictly less than $n^{1/3}$. But p was the smallest prime divisor of n, and it was greater than $n^{1/3}$, so this is a contradiction.

5. We first note that for any n, by the geometric sum formula, we have

$$2^n - 1 = \sum_{k=0}^{n-1} 2^k = 2^{n-1} + 2^{n-2} + \cdots + 4 + 2 + 1.$$

We will show that if n is composite we can always factor the sum on the right.

Suppose that n is composite. In that case there are integers a and b with $1 < a \leq b < n$ such that $n = ab$. Then the sum $\sum_{k=0}^{n-1} 2^k$ has $n = ab$ terms, which can be "split up" in the following way:

$$\begin{aligned}
\sum_{k=0}^{n-1} 2^k &= 2^{n-1} + 2^{n-2} + \cdots + 4 + 2 + 1 \\
&= (2^{ab-1} + 2^{ab-2} + \cdots + 2^{(a-1)b+1} + 2^{(a-1)b}) + \cdots \\
&\quad + (2^{2b-1} + 2^{2b-2} + \cdots + 2^{b+1} + 2^b) + (2^{b-1} + 2^{b-2} + \cdots + 2 + 1) \\
&= \sum_{k=0}^{a-1} \sum_{j=0}^{b-1} 2^{bk+j}.
\end{aligned}$$

We note that term in the "split up" sum factors as

$$\sum_{j=0}^{b-1} 2^{bk+j} = 2^{bk} \sum_{j=0}^{b-1} 2^j.$$

Therefore if we factor by grouping, we get that

$$\begin{aligned}
\sum_{k=0}^{n-1} 2^k &= \sum_{k=0}^{a-1} \sum_{j=0}^{b-1} 2^{bk+j} \\
&= \sum_{k=0}^{a-1} \left(2^{bk} \sum_{j=0}^{b-1} 2^j \right) \\
&= \sum_{k=0}^{a-1} 2^{bk} \cdot \sum_{j=0}^{b-1} 2^j.
\end{aligned}$$

To prove that $2^n - 1$ is composite, it now suffices to show that neither of these two sums is 1. Since they are each sums of positive integers, it suffices to show that neither is a sum containing only the single term 1. Since both a and b are strictly greater than 1, each sum always contains at least two terms (the terms where $k = 0$ and where $k = 1$) and therefore each sum is at least 2. This gives a non-trivial factorization of $2^n - 1$ when n is composite, which proves that $2^n - 1$ is itself composite.

The converse, however, is not true. If $p = 11$, then $2^{11} - 1 = 2047 = 23 \cdot 89$.

Much simpler proof provided by a student, but uses modular arithmetic: Let n be a composite number. By definition, there exist integers a and b with $1 < a \leq b < n$ such that $n = ab$.

We first prove that $2^b - 1$ divides $2^n - 1$, by proving that $2^n - 1 \equiv 0 \pmod{2^b - 1}$. (Note that this is also what the other proof ended up showing, since $2^b - 1 = \sum_{j=0}^{b-1} 2^j$.)

To do this, we begin by noting that $2^b - 1 \equiv 0 \pmod{2^b - 1}$, since $2^b - 1$ divides itself. Therefore, by Lemma 1, part d), we have that $2^b \equiv 1 \pmod{2^b - 1}$.

Now using Lemma 1, part e) repeatedly, we can show that

$$2^n = (2^b)^a \equiv 1^a = 1 \pmod{2^b - 1},$$

which simplifies to saying that $2^n \equiv 1 \pmod{2^b - 1}$. Again using Lemma 1 part d), we may write

$$2^n - 1 \equiv 0 \pmod{2^b - 1},$$

which proves that $2^b - 1$ divides $2^n - 1$.

To conclude that $2^n - 1$ is composite, it now suffices to show that $2^b - 1$ is not 1 or $2^n - 1$. To prove the first assertion, it suffices to note that we have assumed that $b \geq 2$, since n is composite, and therefore $2^b - 1 \geq 3$. To prove the second assertion, we notice that we assumed that $b < n$. Therefore $2^n - 1$ has a non-trivial divisor and it is not prime.

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100
101	102	103	104	105	106	107	108	109	110
111	112	113	114	115	116	117	118	119	120
121	122	123	124	125	126	127	128	129	130
131	132	133	134	135	136	137	138	139	140
141	142	143	144	145	146	147	148	149	150
151	152	153	154	155	156	157	158	159	160
161	162	163	164	165	166	167	168	169	170
171	172	173	174	175	176	177	178	179	180
181	182	183	184	185	186	187	188	189	190
191	192	193	194	195	196	197	198	199	200