Math 40520 Theory of Number
Homework 5

Due Wednesday, 2015-10-07, in class

Do 5 of the following 8 problems. Please only attempt 5 because I will only grade 5.

1. Compute $\binom{194871}{1610}$ mod 385. [Hint: Use our theorem for binomial coefficients modulo primes (Lucas' theorem) and the Chinese Remainder Theorem.]

Proof. **First solution:** Note that

$$\begin{aligned} 194871 &= 22213441_{(5)} & \qquad 1610 &= 22420_{(5)} \\ 194871 &= 1441065_{(7)} & 1610 &= 4460_{(7)} \\ 194871 &= 123456_{(11)} & 1610 &= 1234_{(11)} \end{aligned}$$

so Lucas' theorem on binomial coefficients mod p yields

$$\begin{aligned} \binom{194871}{1610} &\equiv \binom{2}{0}\binom{2}{0}\binom{1}{2}\binom{3}{2}\binom{4}{4}\binom{4}{2}\binom{1}{0} \equiv 0 \pmod 5 \\ \binom{194871}{1610} &\equiv \binom{1}{0}\binom{4}{0}\binom{4}{0}\binom{1}{4}\binom{0}{4}\binom{6}{6}\binom{5}{0} \equiv 0 \pmod 7 \\ \binom{194871}{1610} &\equiv \binom{1}{0}\binom{2}{0}\binom{3}{1}\binom{4}{2}\binom{5}{3}\binom{6}{4} \\ &\equiv 1 \cdot 1 \cdot 3 \cdot 6 \cdot 10 \cdot 15 = 2700 \equiv 5 \pmod{11} \end{aligned}$$

Thus the binomial is $S \equiv 0 \pmod{35}$ and $S \equiv 5 \pmod{11}$. The CRT, using $-5 \cdot 35 + 16 \cdot 11 = 1$, then yields $S \equiv -175 \cdot 5 \equiv 280 \pmod{385}$.

Second solution: Note that $\binom{194871}{1610} = 66122324608730751026639340668325632548050901293488$
57823002530682859250228353922756499936960511349560070624233100740985617270286909222221264
36941053960679756394462708622850051410770472601850848885332896004233703242468461545289438
31974607922017994716250895503012302076504838908584368030857600975645858287955334282411520
41743997139294946212949149548011836215937128198663253527381217454702076765841117452443549
24664026006834319380528493177505181957365774564184456571972880284324670220875840163871589
07580604618066492377115058931414003114699633953377300913756138433023852849063081610866517
00540070855373480742019362435304036495213287033241292532305546149315737008946071714720395
56907219833878827467898201293391113420188683475869351378338631437097094754334849934755192
53424051680203223246569684845731614720201039398578437158162037474579136890740064226583639
06856149885909581634770043880274755897763972645541578946172838087377143863385675600913446
69469379379089122076764831802847405081172966109479053823339120351971402310280166781321 46

882283171381667130497234063939932679921409160768329362048085955062315113216863806258565930167320957681439711621351513389525738281851553845314934100422913697446760114268656333703258292825562631477308216159660313228275262068427270758017196095731752702371903635682479532590533603929764689301534157841023978155668455819430426508887182614891095671169740044666554273570085202747193756845871275969023346105758521748791770000601831684204021562143405841523755679557149307314843562823607174671403150927069180904662830559579461432054116159729554567167832985014205141716082853736414954461916675372661033964950813427590151097620810459951691055278074876974198277283315216115655137571735884812030238070269107737050394784012483253838420413095060386328448307025662299354058732164553240741517355565727596592285241821092742490859461000701351935173840921220769846856900312608584130613004033647059618637316750944167280831755117626591594437777178402839777433353915183940489453624590498615797831359935093430974495850673735509741405751091100567607402125110040530942780120109731730370432543914497211829667476015954860016484975705831556644100717610893564228196128829253940073224136864163846329161605691765216449281398908591405243143686631212416911294649390474986593048631422698274042401437279034729757840816573315309104987236819516151896453986927084357709581548640410746833170243440949779261093838825581532594079337952968433840866406426094994357942331229813427595535001295382228466910948012788313022024002723588177462082147723220153872898599456990101597674851448672594847688560663158715529245095218215424406068728683288589622752210134882284488553250633829691001909659836273890769482712349214335128553503902197085317772330922606491989307149370126062399878327716768418552022658436480697628404652332736206934896799476770146225621022646788335775224053568883727323717717458041772787068549890524786235057279387760409159699464666738021620152802378028608177395839167611482934650285859642777086260598171708324128100795078546840324417938770966259122164110955350732588377133571795985659615424323992353881281461360447864982084316056496558431110367063592678873957437816536748730656050694280482763965960481270341660319390841446063118424632978972145624281053588920883861353561880031033308801151863544612399356241671379516161158338474362935850147031037635247541111403518947843368314260700552706127114041216521063670383624078207705860745877737713408033754973496037123774531960194597310965105343260599694659681616633801407893761626910701228928493764020842879974766603210570676390565884370970997042533502118583202981058961344410058958668937354581248603613553132159631141918288370884894733585532976612074995449790849877188963744885205389479127833624116315813426537760089461134297556676671975576517089042903877110100956691001757190978620863716233413145873604365927166506108000659185163289168820608820571653026945830649030999744950667030534239804040771455626176361502406495908402758091958768517485121650885857745683695450766280861736555461524355629470892596743344 and this is $\equiv 280 \pmod{385}$.

□

2. (This is a more sophisticated looking, yet easier, version of the previous problem.) A *Sophie-Germaine* prime is a prime p such that $q = 2p + 1$ is also a prime (conjecturally there are infinitely many such primes, the largest known having about 200k digits). Suppose $p \geq 7$ is a Sophie-Germaine prime and $q = 2p + 1$. Show that

$$\binom{pq + pq^2}{pq} \equiv 30q - 2p \equiv 58p + 30 \pmod{pq}$$

[Hint: Same as for the previous problem, but it's easier to write down the digits in bases p and q.]

Proof. In base q things are straightforward as $pq + pq^2 = \overline{pp0}_{(q)}$ and $pq = \overline{p0}_{(q)}$ since $p < q$ is a digit in base q. In base p, q is not a digit but

$$pq + pq^2 = p(2p + 1) + p(2p + 1)^2 = 4p^3 + 6p^2 + 2p = \overline{4620}_{(p)}$$

and $pq = 2p^2 + p = \overline{210}_{(p)}$.

Therefore, writing S for the binomial, we have

$$S \equiv \binom{p}{0}\binom{p}{p}\binom{0}{0} \equiv 1 \pmod{q}$$
$$S \equiv \binom{4}{0}\binom{6}{2}\binom{2}{1}\binom{0}{0} \equiv 30 \pmod{p}$$

Bezout is simple as $-2p + q = 1$ so CRT yields

$$S \equiv 1 \cdot (-2p) + 30 \cdot q = 30q - 2p = 58p + 30 \pmod{pq}$$

□

3. Compute

$$12^{34^{56^{78}}} \mod 90$$

[Hint: It is much easier to use Euler's theorem in conjunction with the Chinese Remainder Theorem.] (The author of this problem was very proud of having used each digit exactly once. This idiosyncrasy actually makes the problem easier.)

Proof. Call N the number. We compute N mod 2, 9 and 5 separately. Clearly $N \equiv 0 \pmod 2$. Since $3 \mid 12$, N is also divisible by $3^{34^{56^{78}}}$ so $N \equiv 0 \pmod 9$. It remains to do mod 5. The exponent $34^{56^{78}}$ is divisible by 4 (in fact by $2^{56^{78}}$). Since $12^4 \equiv 1 \pmod 5$ we deduce that $N \equiv 1 \pmod 5$. So $N \equiv 0 \pmod{18}$ and $N \equiv 1 \pmod 5$. CRT then yields $N \equiv 36 \pmod{90}$. □

4. Let n be a number such that $n + 1$ is divisible by 24. If $d \mid n$ show that 24 divides $d^2 - 1$.

Proof. It suffices to show that $3 \mid d^2 - 1$ and $8 \mid d^2 - 1$. Write $n = 24k - 1$ in which case $d \mid 24k - 1$ implies that $3 \nmid d$ and we've already seen that in that case $d^2 \equiv 1 \pmod 3$. Also d is odd so $d \bmod 8 \in \{\pm 1, \pm 3\}$ in which case we immediately see that $d^2 \equiv 1 \pmod 8$. Putting everything together (with CRT if you must) if 3 and 8 divide $d^2 - 1$ it follows that $24 \mid d^2 - 1$. □

5. Exercise 4.19 on page 82.

Proof. It suffices to solve $x^{18} + 4x^{14} + 3x + 10 \equiv 0$ modulo 3 and 7 separately. Mod 3 we can manually check $x = 0, 1, 2$ to see that $x = 1, 2$ work. Mod 7 we note that $x = 0$ does not work. If x is a root it must be nonzero in which case Fermat's little theorem yields $x^6 \equiv 1 \pmod 7$. But that $x^{18}+4x^{14}+3x+10 \equiv 1+4x^2+3x+10 \equiv 4x^2-4x+4 \pmod 7$. In $\mathbb{R}$ we have $x^2-x+1 = (x-1/2)^2+3/4$ which mod 7 has the pleasant form $x^2 - x + 1 \equiv (x-4)^2 - 1 \pmod 7$ as $2^{-1} = 4 \pmod 7$. Thus there are two roots, namely $x = 4 \pm 1 \pmod 7$ so $x \equiv 3, 5 \pmod 7$.

For each of the two roots mod 3 and each of the two roots mod 7 we get a root mod 21 via CRT, for a total of 4 roots. Bezout is $-6 + 7 = 1$ so the solutions are

$$x \equiv 7 \cdot 1 - 6 \cdot 3 \equiv 10 \pmod{21}$$
$$x \equiv 7 \cdot 1 - 6 \cdot 5 \equiv 19 \pmod{21}$$
$$x \equiv 7 \cdot 2 - 6 \cdot 3 \equiv 17 \pmod{21}$$
$$x \equiv 7 \cdot 2 - 6 \cdot 5 \equiv 5 \pmod{21}$$

□

6. Exercise 5.8 on page 90.

Proof. Write $n = p_1^{n_1} \cdots p_k^{n_k}$ with $p_1 < \ldots < p_k$ primes. Then we need to show that

$$\varphi(n) = p_1^{n_1-1}(p_1-1)\cdots p_k^{n_k-1}(p_k-1) = m$$

has finitely many solutions. Since $p_k - 1 \leq \varphi(n)$ it follows that $p_k \leq 1 + m$ so the largest possible prime divisor of n is bounded by $m+1$. This implies that there are only finitely many possible prime divisors of n each each such prime divisor will then have to be $\leq m+1$. Also note that for each i, $p_i^{n_i-1} < \varphi(n) = m$ and so $n_i < 1 + \log_{p_i}(m)$ which implies that for each of these finitely many prime divisors of n, only finitely many exponents are possible. This implies that finitely many n exist such that $\varphi(n) = m$. □

7. Exercise 5.9 on page 90.

Proof. We need to find $n = p_1^{n_1} \cdots p_k^{n_k}$ smallest such that

$$\frac{\varphi(n)}{n} = \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right) < \frac{1}{4}$$

Since the exponents do not show up in the condition we may choose them to be all 1 so we seek the smallest $n = p_1 \cdots p_k$ a product of distinct primes with this condition. As $1 - 1/x$ is an increasing function with values < 1 when x is positive to make the expression $\prod(1 - 1/p_i)$ we need to make the primes p_i as small as possible. So the smallest value is obtained when $p_1 = 2$, $p_2 = 3$, etc. We see that

$$\begin{aligned}
\frac{\varphi(2)}{2} &= \frac{1}{2} \\
\frac{\varphi(2\cdot 3)}{6} &= \frac{1}{3} \\
\frac{\varphi(2\cdot 3\cdot 5)}{30} &= \frac{4}{15} > \frac{1}{4} \\
\frac{\varphi(2\cdot 3\cdot 5\cdot 7)}{210} &= \frac{8}{35} < \frac{1}{4}
\end{aligned}$$

so the smallest n is $n = 210$. □

8. Exercise 5.21 on page 96.

Proof. Write $n = p_1^{n_1} \cdots p_k^{n_k}$ and rearrange the primes in such a way that the divisor $d = p_1^{m_1} \cdots p_r^{m_r}$ is only divisible by the first r prime factors of n. The exponents are then $m_1 \leq n_1, \ldots, m_r \leq n_r$. But then

$$\begin{aligned}
\frac{\varphi(n)}{\varphi(d)} &= \frac{p_1^{n_1-1}(p_1-1)}{p_1^{m_1-1}(p_1-1)} \cdots \frac{p_r^{n_r-1}(p_r-1)}{p_r^{m_r-1}(p_r-1)} \cdot \frac{p_{r+1}^{n_{r+1}-1}(p_{r+1}-1)}{1} \cdots \frac{p_k^{n_k-1}(p_k-1)}{1} \\
&= \prod_{i=1}^{r} p_i^{n_i-m_i} \prod_{i=r+1}^{k} p_i^{n_i-1}(p_i-1)
\end{aligned}$$

which is an integer. □