MIDTERM EXAM SOLUTIONS
MATH 115: NUMBER THEORY

Problem 1. We compute

$$\begin{aligned} 2004 &= 20 \cdot 99 + 24 \\ 99 &= 4 \cdot 24 + 3 \\ 24 &= 3 \cdot 8 + 0 \end{aligned}$$

so $\gcd(2004, 99) = 3$.

For (b), we work backwards:

$$3 = 99 - 4 \cdot 24 = 99 - 4(2004 - 20 \cdot 99) = -4 \cdot 2004 + 81 \cdot 99.$$

Problem 2. By unique factorization, we may write

$$a = p_1^{e_1} \dots p_r^{e_r}, \qquad b = p_1^{f_1} \dots p_r^{f_r}$$

where $e_i, f_i \geq 0$ are nonnegative integers and the p_i are primes. We know that

$$p_1^{3e_1} \dots p_r^{3e_r} = a^3 = b^2 = p_1^{2f_1} \dots p_r^{2f_r}$$

so again by unique factorization, we know that $3e_i = 2f_i$ for all i.

Since $2 \mid (2f_i)$ we know $2 \mid (3e_i)$ so since $\gcd(2, 3) = 1$ (or since 2 is prime and $2 \nmid 3$), we know $2 \mid e_i$. Let $e_i = 2c_i$, and let $d = p_1^{c_1} \dots p_r^{c_r}$. Then clearly $d^2 = a$. Moreover, $3e_i = 6c_i = 2f_i$ so $3c_i = f_i$. Therefore

$$d^3 = p_1^{3c_1} \dots p_r^{3c_r} = p_1^{f_1} \dots p_r^{f_r} = b$$

as well.

Here is a second proof: like in homework, since $a^3 = b^2$ we know $a^3 \mid b^2$ hence $a \mid b$, so $b/a = d \in \mathbb{Z}$ is an integer. Already $d^3 = b^3/a^3 = b^3/b^2 = b$ and $d^2 = b^2/a^2 = a^3/a^2 = a$.

Problem 3. We first find a solution to

$$x^2 - 7x - 6 \equiv 0 \pmod 3$$

i.e.

$$x^2 - x \equiv 0 \pmod 3.$$

This has the solutions $x \equiv 0, 1 \pmod 3$.

Start with $r_0 = 0$ and use Hensel's lemma (Newton's method). Let $f(x) = x^2 - 7x - 6$, so then $f'(x) = 2x - 7$. Then

$$f'(0) = -7 \equiv -1 \not\equiv 0 \pmod 3$$

so there exists a unique lift of this solution modulo 3^3 (indeed, to any power 3^i). We find

$$f'(r_0)^{-1} \equiv (-1)^{-1} \equiv -1 \pmod 3$$

so

$$r_1 = r_0 - f(r_0)(f'(r_0) \bmod 3)^{-1} = 0 + (-6) \equiv 3 \pmod 9$$

Date: July 15, 2004.

and similarly

$$r_2 = 3 + (-18) \equiv 12 \pmod{27}.$$

We check that indeed $12^2 - 7(12) - 6 \equiv 0 \pmod{27}$. The other solution $x \equiv 1 \pmod 3$ lifts to $x \equiv 22 \pmod{27}$.

For part (b), we note that since $f'(0), f'(1) \not\equiv 0 \pmod 3$, by Hensel's lemma we can lift these solutions modulo 3 to a unique solution modulo $3^5 = 243$, so there are exactly two solutions.

Problem 4. Since 365 is odd and 94 is even, n is odd so $2 \nmid n$.

We find that $365 \equiv 2 \pmod 3$ and $94 \equiv 1 \pmod 3$, so

$$n \equiv 2^{2004} + 1 \pmod 3.$$

Now $2^2 = 4 \equiv 1 \pmod 3$, so

$$n \equiv 2^{2 \cdot 1002} + 1 \equiv 1 + 1 \not\equiv 0 \mod 3$$

so $3 \nmid n$.

Since $5 \mid 365$ but $5 \nmid 94$, we see $5 \nmid n$.

Since $365 \equiv 1 \pmod 7$ we have

$$n \equiv 1^{2004} + 94 \equiv 1 + 3 \not\equiv 0 \pmod 7$$

so $7 \nmid n$.

Finally, $365 \equiv 2 \pmod{11}$. Since $\gcd(2, 11) = 1$, by Fermat's little theorem, we have $2^{10} \equiv 1 \pmod{11}$. Hence

$$n \equiv 2^{2000+4} + 6 \equiv 1 \cdot 16 + 6 = 22 \equiv 0 \pmod{11}$$

so $11 \mid n$ and 11 is the smallest prime divisor.

Problem 5 (Bonus). We draw a right triangle with interior angle α: the statement $\arctan(7/2) = \alpha$ says that the opposite side to the angle α has length 7 and the adjacent side has length 2. By the Pythagorean theorem, this implies that the hypotenuse has length $\sqrt{7^2 + 2^2} = \sqrt{53}$, hence $\beta = \sin(\alpha) = 7/\sqrt{53} = (7/53)\sqrt{53}$.

First note that $\sqrt{53}$ is irrational. There are many possible proofs of this fact, one goes as follows: if $\sqrt{53} = a/b$, with $\gcd(a, b) = 1$, then $53b^2 = a^2$, so

$$\mathrm{ord}_{53}(53b^2) = 1 + 2\,\mathrm{ord}_{53}(b) = 2\,\mathrm{ord}_{53}(a),$$

a contradiction since an integer cannot both be even and odd. But this also shows that β is irrational, since if $(7/53)\sqrt{53} = c/d$ then $\sqrt{53} = (53c)/(7d) \in \mathbb{Q}$, a contradiction.