UNIQUE FACTORIZATION AND FERMAT'S LAST THEOREM
HOMEWORK 2

The main purpose of this homework assignment is to use the existence of unique factorizations of 3-cyclotomic integers to prove Fermat's Last Theorem in the case $n = 3$. The arguments, while beautiful, are quite involved. I recommend starting with Problems 1 and 3, and coming back to Problem 2 (which is much easier than Problem 3) if you have the time and inclination.

We begin with one last reduction step. Suppose that there exist nonzero integers x, y, z such that

$$x^3 + y^3 = (x+y)(x+\zeta y)(x+\zeta^2 y) = z^3. \tag{0.1}$$

If a prime p divides two of x, y, z, then it divides the third, and

$$\left(\frac{x}{p}\right)^3 + \left(\frac{y}{p}\right)^3 = \left(\frac{z}{p}\right)^3.$$

Replacing x, y, z with $x/p, y/p, z/p$ and continuing in this fashion, we may assume that x, y, z are *pairwise coprime*, i.e. that any two of x, y, z are coprime.

Problem 1 (The greatest common divisor of $x+y, x+\zeta y, x+\zeta^2 y$). Let $x, y \in \mathbf{Z}[\zeta]$ be nonzero coprime 3-cyclotomic integers.

(i) Using the fact that x and y are coprime, show that there exist $c_1, c_2, c_3, d_1, d_2, d_3 \in \mathbf{Z}[\zeta]$ such that

$$\begin{aligned} c_1(x+y) + d_1(x+\zeta y) &= \zeta - 1 \\ c_2(x+y) + d_2(x+\zeta^2 y) &= \zeta - 1 \\ c_3(x+\zeta y) + d_3(x+\zeta^2 y) &= \zeta - 1. \end{aligned} \tag{1.1}$$

[Hint: $(x+\zeta y) - (x+y) = (\zeta - 1)y$ and $\zeta(x+y) - (x+\zeta y) = (\zeta - 1)x$.]

(ii) Use (i) to show that the greatest common divisor of any two of the terms $x+y, x+\zeta y, x+\zeta^2 y$ is either $\zeta - 1$ or 1.

(iii) Suppose that $(\zeta - 1) \nmid (x^3 + y^3)$. Show that $x+y, x+\zeta y$, and $x+\zeta^2 y$ are pairwise coprime.

(iv) Now suppose that $(\zeta - 1) \mid (x^3 + y^3)$. Show that $\zeta - 1$ divides each of the factors $x+y, x+\zeta y$, and $x+\zeta^2 y$, so that the greatest common divisor of any two is equal to $\zeta - 1$ by (ii).

Problem 2 (Fermat's Last Theorem for $n = 3$, "easy" case). Suppose that there exist nonzero *pairwise coprime* integers x, y, z such that $x^3 + y^3 = z^3$. Assume for this problem that $3 \nmid xyz$, so that $x+y, x+\zeta y$, and $x+\zeta^2 y$ are pairwise coprime by Problem 1(iii)[1]. The following is based on a proof due to Sophie Germain.

(i) Note that $x^3 + y^3 = (x+y)(x^2 - xy + y^2)$. Use Problem 1(iii) to show that $x+y$ and $x^2 - xy + y^2$ are coprime *integers*. Conclude using (0.1) that $x+y$ and $x^2 - xy + y^2$ are cubes.

(ii) Replacing z with $-z$, we rewrite our supposed solution in the more symmetric form $x^3 + y^3 + z^3 = 0$. Taking advantage of this symmetry and applying (i), we find that there are integers $a, \alpha, b, \beta, c, \gamma$ such that

$$\begin{aligned} x + y &= a^3 & x^2 - xy + y^2 &= \alpha^3 \\ x + z &= b^3 & x^2 - xz + z^2 &= \beta^3 \\ y + z &= c^3 & y^2 - yz + z^2 &= \gamma^3. \end{aligned}$$

[1] As discussed in class, 3 divides the integer z^3 if and only if $(\zeta - 1) \mid z^3$).

Reducing the equation $x^3 + y^3 + z^3 = 0$ modulo 7, prove that $7 \mid xyz$. Assume without loss of generality that $7 \mid x$. Since

$$a^3 + b^3 + (-c)^3 = 2x \equiv 0 \pmod 7,$$

we have that $7 \mid abc$ for the same reason. Prove that $7 \nmid a$ and $7 \nmid b$, so that $7 \mid c$.

(iii) Since $7 \mid c$ we have $y \equiv -z \pmod 7$, so since $x \equiv 0 \pmod 7$, the above equations give $\gamma^3 \equiv 3\beta^3 \pmod 7$. Use this to show that $7 \mid z$, and derive a contradiction to the assumption that x, y, z are pairwise coprime.

Problem 3 (Fermat's Last Theorem for $n = 3$, hard case). Suppose that there exist nonzero pairwise coprime integers x, y, z such that $x^3 + y^3 = z^3$, and assume now that $3 \mid xyz$. If $3 \mid x$ then we can rewrite (0.1) as $(-z)^3 + y^3 = (-x)^3$; replacing x with $-z$ and z with $-x$, and using a similar trick if $3 \mid y$, we may assume without loss of generality that $3 \mid z$, so $3 \nmid xy$. The following is based on Kummer's proof of Fermat's Last Theorem in this case, specialized to the exponent 3 (so yes, this proof generalizes enormously). You will in fact prove the following (slightly) more general theorem:

Theorem 3.1. *Let $x, y, w \in \mathbf{Z}[\zeta]$ be pairwise coprime nonzero 3-cyclotomic integers such that $(\zeta - 1) \nmid xyw$, let k be a positive integer, and let $e \in \mathbf{Z}[\zeta]^\times$ be a 3-cyclotomic unit. Suppose that*

$$x^3 + y^3 = e\,(\zeta - 1)^{3k}\, w^3.$$

Then $k > 1$, and there exist pairwise coprime nonzero 3-cyclotomic integers $X, Y, W \in \mathbf{Z}[\zeta]$ such that $(\zeta - 1) \nmid XYW$, a positive integer $K < k$, and a 3-cyclotomic unit $E \in \mathbf{Z}[\zeta]^\times$, satisfying the equation

$$X^3 + Y^3 = E\,(\zeta - 1)^{3K}\, W^3.$$

(i) Show that Theorem 3.1 implies Fermat's Last Theorem in this case.

(ii) Let $a \in \mathbf{Z}[\zeta]$. We say that $z, w \in \mathbf{Z}[\zeta]$ are *congruent modulo a*, and we write $z \equiv w \pmod a$, provided that $a \mid (z - w)$. This definition allows us to do modular arithmetic in $\mathbf{Z}[\zeta]$ in exactly the same way as we do modular arithmetic in the integers.

Prove that any element of $\mathbf{Z}[\zeta]$ is congruent to $0, 1$, or -1 modulo $\zeta - 1$.

(iii) We have a factorization

$$e(\zeta - 1)^{3k} w^3 = (x + y)(x + \zeta y)(x + \zeta^2 y).$$

By Problem 1(iv), $\zeta - 1$ divides all three of the factors on the right side of the above equation, and the greatest common divisor of any two is equal to $\zeta - 1$. We claim that $(\zeta - 1)^2$ divides one (and hence exactly one) of the factors $x + y, x + \zeta y, x + \zeta^2 y$. Writing $x + y = r(\zeta - 1)$ for $r \in \mathbf{Z}[\zeta]$, show that

$$\begin{aligned} x + y &= (\zeta - 1)r \\ x + \zeta y &= (\zeta - 1)(r + y) \\ x + \zeta^2 y &= (\zeta - 1)(r - \zeta^2 y). \end{aligned}$$

Use (ii) and the fact that $y \not\equiv 0 \pmod{\zeta - 1}$ to prove that $\zeta - 1$ divides one of the terms r, $r + y$, $r - \zeta^2 y$. Conclude that $(\zeta - 1)^4 \mid (x^3 + y^3)$, so $k > 1$, and that $(\zeta - 1)^{3k-2}$ divides one of the factors $x + y, x + \zeta y, x + \zeta^2 y$.

(iv) Let $K = k - 1 > 0$. If $(\zeta - 1)^{3k-2}$ divides $x + \zeta y$ (resp. $x + \zeta^2 y$), replace y with ζy (resp. $\zeta^2 y$) so that $(\zeta - 1)^{3k-2} = (\zeta - 1)^{3K+1}$ divides $x + y$. Show that

$$\begin{aligned} x + \zeta^{-1} y &= (\zeta - 1)\, e_{-1}\, t_{-1}^3 \\ x + y &= (\zeta - 1)\, e_0\, (\zeta - 1)^{3K}\, t_0^3 \\ x + \zeta y &= (\zeta - 1)\, e_1\, t_1^3 \end{aligned} \tag{3.1}$$

for some units $e_{-1}, e_0, e_1 \in \mathbf{Z}[\zeta]^\times$, and pairwise coprime nonzero 3-cyclotomic integers $t_{-1}, t_0, t_1 \in \mathbf{Z}[\zeta]$ not divisible by $\zeta - 1$. (Note that $\zeta^{-1} = \zeta^2$.)

(v) Eliminate x and then y from (3.1) to obtain

$$0 = e_1 t_1^3 - (1+\zeta)e_0(\zeta-1)^{3K}t_0^3 + e_{-1}t_{-1}^3.$$

Divide through by e_1 to get the relation

$$E_0(\zeta-1)^{3K}t_0^3 = t_1^3 + E_{-1}t_{-1}^3, \tag{3.2}$$

where $E_0, E_{-1} \in \mathbf{Z}[\zeta]^\times$ are units (why?).

(vi) Show that for any $a \in \mathbf{Z}[\zeta]$, its cube is a 3-cyclotomic integer congruent to $0, 1$, or -1 modulo 3, and that $a^3 \equiv 0 \pmod 3$ if and only if $(\zeta-1) \mid a$. Prove that the unit E_{-1} in (3.2) is congruent to $0, 1$, or -1 modulo 3, and use this to show that $E_{-1} = \pm 1$. Now rewrite (3.2) in the required form of Theorem 3.1.

(vii) Other than the (critically important) fact that $\mathbf{Z}[\zeta]$ has unique factorizations, can you determine which step in the above proof is by far the hardest to generalize to odd prime exponents $p > 3$? (I will be impressed if you figure out.)

Problem 4. Prove "by hand" that 2 is prime in $\mathbf{Z}[\zeta]$.